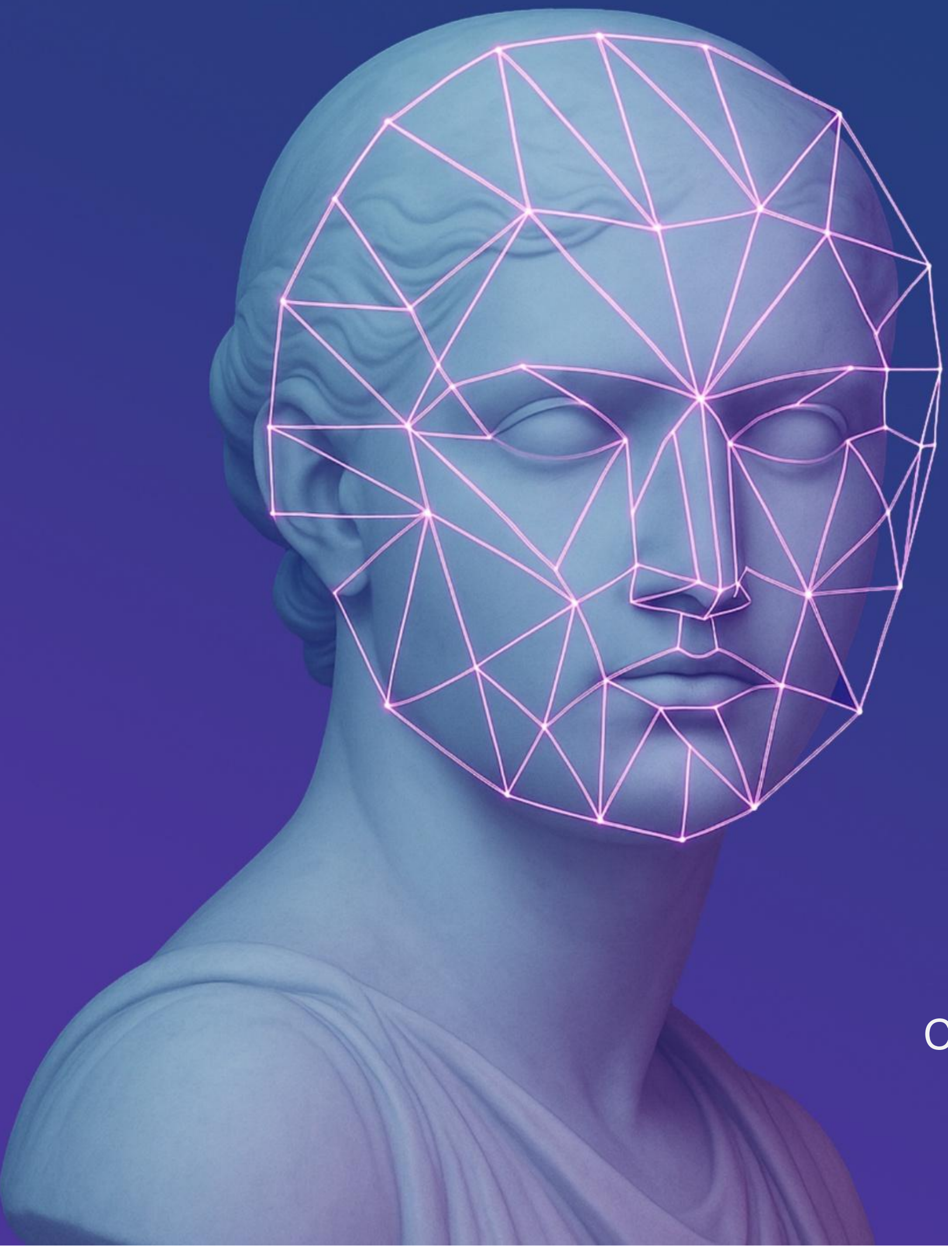
Fraud in the Digital Age

Independent Review of Disclosure and Fraud Offences

Jonathan Fisher KC



CP 1600

Government of the United Kingdom
Home Office

Fraud in the Digital Age

Independent Review of Disclosure and Fraud Offences

Presented to Parliament
by the Secretary of State for the Home Department
by Command of His Majesty

July 2026

CP 1600

This publication is available at: https://www.gov.uk/official-documents

Any enquiries regarding this publication should be sent to us at https://www.gov.uk/guidance/contact-the-home-office

ISBN - 978-1-5286-6210-9
E03539408 07/26

Printed on paper containing 40% recycled fibre content minimum

Printed in the UK by HH Associates Ltd. on behalf of the Controller of His Majesty’s Stationery Office
.

Contents

Foreword......2
Executive Summary......4
1. Introduction......10
2. A Short History of Fraud......15
3. Contemporary Picture......36
4. Enablers and Connected Criminality......44
5. Legislative Landscape......52
6. Corporate Responsibility......63
7. Emerging Threats and Satellite Offences......77
8. Detection and Disruption......92
9. Public–Private Partnerships......99
10. Data-Sharing......111
11. Whistleblower Incentivisation......125
12. Investigation......143
13. Powers......156
14. International Cooperation......174
15. Prosecution......184
16. Courts......190
17. Penalties and Remedies......208
18. Rehabilitation......234
19. Victims......240
20. Education and Awareness......249
21. Conclusion......253
22. List of Recommendations......255
23. Annex A – Terms of Reference......262
24. Annex B – Governance......264
25. Annex C – Summary of Engagement......265
26. Annex D – Glossary......268

Cover illustration: The image depicts a contemporary interpretation of *Apate*, the ancient Greek personification of deceit and fraud, created in part with artificial intelligence. This design symbolises the enduring nature of deceptive behaviours, now reimagined in the digital age.

Foreword

Fraud has grown exponentially in the last 20 years. With annual losses caused by fraud estimated at £2.3 billion,[1] it is no exaggeration to describe fraud as the criminal scourge of our age. It accounts for 44% of criminal surveyed activity,[2] within which 80% is attributable to digital and internet-facilitated fraud.[3]

The impact of fraud is not limited to losses suffered by innocent victims, whether individuals or companies, or financial damage inflicted on the economy at large. As an offence committed covertly and not openly, fraud scars many of its victims with serious emotional and psychological harm resulting from the breach of trust between victim and perpetrator which has taken place.[4] In *Dante's Inferno*, the ninth Circle of Hell, the deepest level, is where the Devil finds himself surrounded by people who betray the trust of others. For Dante, the worst violation of moral behaviour is treachery.

More fundamentally, honest dealings are essential for a society to rest on secure foundations. Fraud is a crime against possession, which infringes autonomy by undermining the right to enjoy property. In consequence, the expectation of trust and security between people which allows a market economy to flourish is denied.

Although historically there has been an ambivalence towards fighting fraud, combating fraud has been higher on Government agendas in recent years. Whilst there is no silver bullet, the recommendations made in this Review will refresh the weaponry in the anti-fraud armoury and introduce new measures appropriate to fighting fraud in a digital age.

Whilst effective criminal prosecution lies at the heart of the response to those who commit fraud, law enforcement cannot simply arrest its way out of this problem. More imaginative measures need to be taken. The thread which connects the 47 recommendations is the principle that the time for tolerating latitude towards fraud has long gone. In the battle against fraud today, zero tolerance is the name of the game.

Acknowledgements

This Review has benefited from extensive engagement across the criminal justice system, law enforcement agencies, regulatory bodies, academia and industry. Evidence was gathered through interviews, written submissions, roundtable discussions and expert panels, each of

[1] RSM UK, 'Fraud loss reaches £2.3bn as fraudsters become increasingly sophisticated', (2025), [Accessed 28 October 2025].
[2] Office for National Statistics, *Statistics on Crime in England and Wales*, (2025), table A1. The Crime Survey for England and Wales (CSEW) measures crimes against people aged 16+ living in private households; it excludes certain offences (e.g. homicide) and crimes against businesses/society.
[3] Cifas, *This is Fraudscape 2025*, (2025), page 1.
[4] Home Office, *Experiences of victims of fraud and cyber crime*, (2025).

which provided perspectives that have materially informed the analysis and recommendations contained in this Review.

I am indebted to all those who contributed their time and expertise so generously. Their insights have been critical in shaping an evidence-led assessment of the issues under consideration. A full list of organisations and individuals consulted during this second phase is set out in Annex C.

I also wish to place on record my particular thanks to Anita Clifford (QEB Hollis Whiteman, London), Alex Davidson (2 Bedford Row, London) and Olivia English (23ES, London) for their invaluable assistance and constructive challenge throughout the course of the second part of this Review, and to the secretariat team, and in particular Tim Craine, for their dedication in supporting its delivery.

Jonathan Fisher KC

Chair of the Independent Review of Disclosure and Fraud Offences

December 2025

Executive Summary

1. Fraud is now one of the defining crimes of the digital age. It is no longer a peripheral offence but a direct threat to personal autonomy, economic stability, and public trust. In England and Wales, fraud may soon constitute half of all crime, with an estimated 4.1 million offences in the year to June 2025.[5] One in 14 adults is a victim of fraud,[6] and one in four businesses experiences fraud annually.[7] Fraud is pervasive.

2. Despite its scale, fraud has historically been treated with indifference. That era must end. This Review was commissioned to examine why the criminal justice system has failed to keep pace with fraud-related offending, and to propose reforms that set a new course as the Government takes the fight to fraud.

3. The objective of this Review is to consider the following questions:

    a. Are the current methods of detection, investigation and prosecution sufficiently robust?

    b. Does the legislative framework possess the flexibility required to respond to modern fraud-related offending?

    c. Do current penalties fit the crime?

4. The findings are stark. Fraud is now one of the most prevalent crimes in the United Kingdom (UK), yet deterrence is almost non-existent. The average victim, who is fortunate enough for their case to be investigated, will have to wait 18 months for a charging decision, almost eight times longer than for the average criminal case.[8] For those cases that do reach court, delay is the norm. A typical serious fraud case takes 442 days from arrival at the Crown Court to completion, twice as long as an ordinary case.[9]

5. This lack of celerity, coupled with near-certain impunity for offenders, creates fertile ground for fraud to flourish as a low-risk, high-reward activity. When only 1% of reported fraud cases result in a criminal justice outcome,[10] the message to offenders is plain: the odds are overwhelmingly in their favour. Even those who have never before contemplated breaking the law may be tempted when the prospect of detection and punishment is remote.

---

[5] Office for National Statistics, *Statistics on Crime in England and Wales*, (2025), table A1.
[6] Ibid. table: A3. Calculated using the number of estimated fraud victims (3.45 million) and prevalence rate (7.1%).
[7] Home Office and Ipsos, *Economic Crime Survey 2024,* (published November 2025), Businesses with employees, paragraph 2.1.
[8] Ministry of Justice, End-to-end timeliness tool, *Criminal court statistics year to March 2025*. 442 days (mean), 236 days (median).
[9] Ibid.
[10] Home Office, *Crime outcomes in England and Wales: 2024to 2025*, year to March 2025, (August 2025), table 5.2.1.

6. Barriers to investigation are formidable. Offenders frequently operate from overseas jurisdictions, placing them beyond the immediate reach of domestic law enforcement. Investigators face mountains of digital material: vast datasets that must be meticulously examined, scheduled, redacted and disclosed in accordance with statutory obligations.[11] These technical demands collide with limited resources, competing operational priorities and a persistent shortage of specialist skills. The challenge of recruiting and retaining experienced financial investigators compounds the problem, many trainee investigators will not see a fraud investigation through to its conclusion before moving to other roles, because such cases are protracted.

7. Taken together, these factors create an environment in which the pursuit of fraud is not merely difficult but structurally constrained, rendering this crime type among the most complex and resource-intensive to investigate and prosecute. It is also costly: the extensive hours invested, the expense of extracting and storing growing volumes of digital material, and the need to employ scarce specialist expertise.

8. The legislative framework itself is broadly sound. The Fraud Act 2006 remains a robust and flexible instrument, capable of addressing a wide range of offending. In addition, the common law offence of conspiracy to defraud retains its importance in complex cases. Ultimately, almost every fraud case, once stripped of technical complexity, turns on whether an individual acted dishonestly, seeking to make a gain or cause a loss. That question remains the fulcrum of every fraud prosecution.

9. Enforcement, however, has been fragmented and sluggish. Corporate and platform accountability is weak. Online platforms host significant scam content, yet bear limited legal liability, while banks shoulder the cost of reimbursing victims. Meanwhile, emerging technologies, artificial intelligence (AI), deepfakes, and crypto-assets, are accelerating the fraud epidemic, equipping criminals to deceive at scale and to launder proceeds with unprecedented ease, frequently from overseas. These activities can now be executed using inexpensive, readily available tools, requiring little or no specialist knowledge. Fraud 'how-to' guides and tools are openly marketed online, as fraudsters instruct one another in effective techniques of deception.[12]

10. Fraud is not a victimless crime. It destroys livelihoods, corrodes trust and inflicts profound emotional harm. The notion that fraud is a mere financial inconvenience is a dangerous mistruth. Victims often suffer lasting psychological damage, and the erosion of trust undermines the foundations on which a market economy depends. Beyond the individual, fraud imposes systemic costs on businesses and the wider economy, diverting resources from productive investment to defensive expenditure and compliance. It is a

---

[11] Home Office, *Disclosure in the Digital Age: Independent Review of Disclosure and Fraud Offences*, (2025), CP 1285.

[12] United Nations Office on Drugs and Crime, *Organized Fraud, Issue Paper,* (2024), pp. 55–57.

drag on competitiveness and a threat to the UK's reputation as a safe and reliable place to do business.

11. The implications are clear—the evolution of the internet and, more recently, AI has ushered in a new era of fraud. Techniques and tools now available to criminals eclipse those of their 20th-century counterparts, creating vulnerabilities on a scale previously unimaginable. It is also transformative in its sophistication, enabling criminals to craft communications that appear convincingly authentic and personally tailored. This shift demands a comprehensive upgrade in anti-fraud measures, reflecting the complexity and reach of digitally enabled crime. While the Review focuses on the downstream delivery of justice after fraud occurs, meaningful reduction must happen upstream.

Recommendations

12. Against this backdrop, incremental adjustments will not suffice. A fundamental recalibration of the State's posture is required, moving from a reactive model, that simply seeks to get victims back on their feet, to a proactive strategy that takes the fight to fraudsters. The recommendations that follow are designed to deliver that shift. They are not cosmetic; they are reforms aimed at restoring deterrence, protecting victims and safeguarding the integrity of the UK economy.

13. First, the Government must simplify and strengthen the data-sharing landscape, or it will find itself chasing shadows. Effective intelligence exchange is the lifeblood of modern fraud detection and prevention. At present, the patchwork of asymmetric provisions leaves fraudsters two steps ahead. If a whole-system model of public–private partnership is to be the vehicle through which modern fraud is combated, it must be built on firm foundations of lawful and confident data-sharing. To that end, intelligence sharing within economic crime-focused public–private partnerships should take place within a statutory framework.

14. Pending legislative improvements, a single memorandum of understanding should be established between public bodies, setting out how data and intelligence can be shared for the purpose of detecting and investigating fraud. The Government, working with the National Crime Agency and Information Commissioner's Office, should issue clear guidance on voluntary and compelled data-sharing, including assurances that lawful sharing will not constitute tipping off or prejudicing an investigation.

15. The law should be updated to give the Serious Fraud Office the same information-sharing powers as the National Crime Agency.[13] More fundamentally, the Government should conduct a full review of all data-sharing rules to ensure they are fit for tackling economic

[13] Crime and Courts Act 2013, s.7.

crime. This will put law enforcement on the front foot and enable real-time disruption of fraud.

16. Second, corporate accountability must be strengthened. The introduction of the 'failure-to-prevent' fraud offence for large organisations under the Economic Crime and Corporate Transparency Act 2023 is a welcome step, but it does not go far enough. The Government should extend existing legislation to expand liability to online platforms whose infrastructure facilitates fraud. The Government should introduce a new corporate criminal offence for providers of regulated user-to-user services, as defined under the Online Safety Act 2023, who fail to prevent fraud on their platforms.

17. Alongside this, an anti-fraud levy should be imposed on digital and communications infrastructure providers, including social media platforms and online service providers, to ensure that those whose systems are exploited contribute proportionately to enforcement and victim support. Funds raised should be ring-fenced for law enforcement capability, public awareness campaigns and technological innovation in fraud detection. These measures will rebalance a system in which banks currently bear the cost of reimbursing victims, while platforms hosting scam content escape liability.

18. Third, the legal framework must be reinforced. The Fraud Act 2006 and the common law offence of conspiracy to defraud remain robust and flexible instruments, and both should be retained. However, some significant gaps exist. Targeted 'satellite' offences should be introduced to address enabling conduct that facilitates fraud but falls short of full-scale offending. These should include summary-only offences for identity theft and deed poll abuse.

19. A multi-pronged enforcement model should be adopted for low-level money laundering, allowing law enforcement to issue warnings, impose civil penalties, or prosecute under the new summary-only offence as appropriate. Guidance should be issued to help officers identify vulnerable individuals who may have been coerced into offending.

20. In addition, law enforcement should be granted powers to issue civil fines to individuals purchasing fraud-enabling products online, mirroring provisions in the Public Authorities (Fraud, Error and Recovery) Act 2025. The Regulation of Investigatory Powers Act 2000 should be amended to reflect modern realities, including clarifying the definition of 'possession' of protected information, expanding appropriate permissions and increasing the maximum term for certain fraud-related disclosure offences.

21. The extraterritorial ambit of section 2(3) of the Criminal Justice Act 1987 should be reviewed to enable the SFO to serve notices on UK directors overseas and foreign corporates with sufficient UK nexus. Also, the sentencing framework for the most serious fraud offences and money laundering should be updated to increase maximum custodial penalties to 20 years, reflecting the gravity and systemic impact of these crimes.

22. Fourth, the Government should build on the recent successes in corralling allies, and, where necessary, unlikely partners, to lead a global coalition against fraud: a crime type that knows no borders. Building on international conventions and resolutions that place fraud in the spotlight, the UK should drive coordinated measures that impose tough consequences on high-harm actors operating outside UK jurisdiction, including targeted sanctions and visa denials.

23. In parallel, the Government should establish fast, lawful channels that enable domestic law-enforcement agencies to swiftly share intelligence with international counterparts and mount joint operations against transnational fraud networks, with clear safeguards and measurable outcomes.

24. The architecture for enforcement and adjudication must be strengthened. The Government should find a consistent mechanism for recording the number of live fraud investigations across all relevant law enforcement agencies and prioritise funding for the deployment of emerging technology, including AI, in proactive detection and disruption.

25. Fifth, court infrastructure must be updated to support the effective trial of complex fraud cases, and the Southwark Protocol should be extended to all Crown Courts hearing serious fraud and economic crime, codifying it into a Judicial Practice Direction. The new Direction should require protected pre-reading days for the trial judge in serious and complex cases, so that they can exercise firm control over disclosure, digital evidence and case management from the outset.

26. Judicial training should be enhanced to address the unique challenges of digital-heavy trials and the emerging threat of AI-enabled fraud. To stop serious fraudsters moving or hiding assets overseas before their trial ends, courts should normally freeze those assets in fraud cases—unless there is a strong reason not to do so.

27. The Government should also reform the early guilty plea framework for complex fraud cases, introducing enhanced judicial indications, increased sentence discounts for very early pleas, and incentives for swift payment of confiscation orders. Deferred Prosecution Agreements should be extended to individuals, with proceeds reinvested into the criminal justice system and a proportion ring-fenced for economic crime enforcement.

28. In parallel, pilots should be launched for diversion schemes and restorative justice programmes in appropriate low-level cases, alongside consideration of civil powers for the Crown Court, to wind up companies used to perpetrate fraud.

29. Sixth, victims and whistleblowers must be placed at the heart of the system. Victims should be clearly informed, through amendment to the Victims' Code, of their right to participate in confiscation proceedings under the Proceeds of Crime Act 2002. The

Serious Fraud Office should be empowered to financially reward whistleblowers, with a consultation launched to design a suitable scheme.

30. Safeguards must include new criminal offences for knowingly making false reports under such a scheme and for harassing or intimidating whistleblowers, as well as the creation of an independent arbitration panel to review complaints.

31. Beyond enforcement, prevention must be embedded upstream. Fraud prevention and ethical awareness should be integrated into the national curriculum, supported by mandatory financial literacy modules for young people opening bank accounts. Public awareness campaigns such as 'Stop! Think Fraud' should be enhanced and targeted at high-risk demographics. Finally, strategic leadership for the Government's fraud response must be prioritised.

Conclusion

32. Fraud cannot be fought by arrests alone. It demands a whole-system response that combines robust enforcement with upstream prevention, corporate responsibility and international cooperation. The recommendations in this Review constitute structural reform, not minor adjustment: they are designed to restore credible deterrence, protect victims and safeguard the integrity of the UK economy.

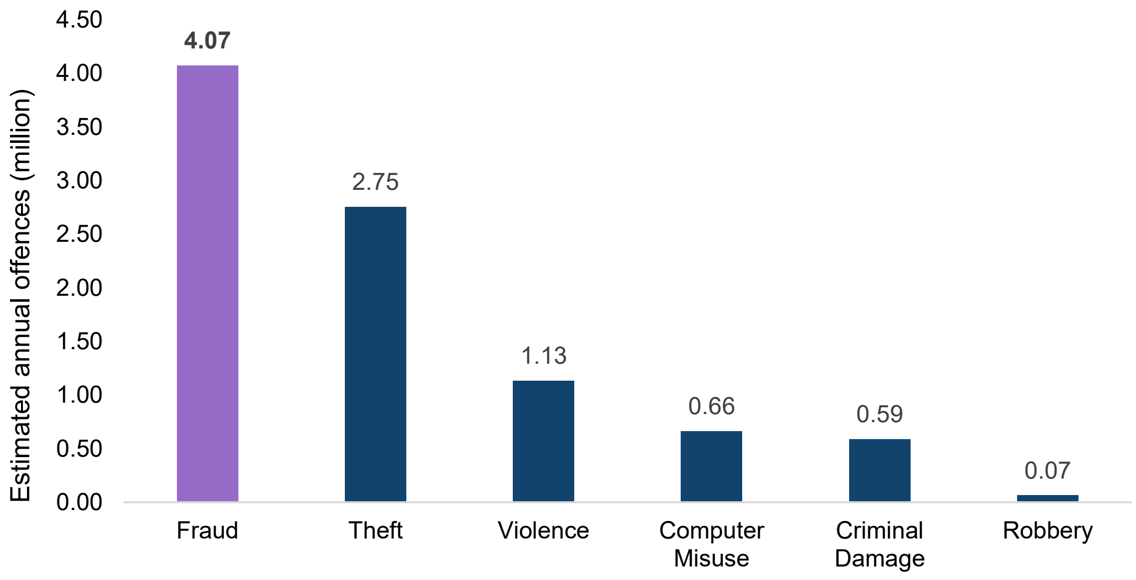
33. The stakes could not be higher. If the Government fails to act decisively, it will sleepwalk into a future where fraud becomes endemic—eroding public trust, undermining autonomy and prosperity, and compromising the rule of law.

1. Introduction

34. The United Kingdom (UK) Government has a fundamental duty to maintain law and order and protect its residents. Controlling crime and upholding justice, for a population of 69.3 million people,[14] is a demanding task, which has become even more difficult since the advent of the internet. Gone are the days when physical proximity to an offender was a key factor in the likelihood of victimisation. No longer do criminals need to be physically present to rob or abuse an individual. Instead, criminals now operate transnationally, ensnaring vulnerable victims from afar, often shielded by the legal protections of foreign jurisdictions.

35. Since the turn of the millennium, one crime has surged ahead of all others—fraud (see figure 1).[15] It is now estimated to account for a staggering 44% of surveyed crime committed in England and Wales, yet has historically received disproportionately little attention in public discourse because, unlike other crime types, it does not 'bang, bleed or shout'.[16] With an estimated 3.45 million victims each year,[17] and one in four business affected,[18] the scale of fraud presents an overwhelming challenge for law enforcement agencies operating with finite resources.

Fig.1 – Fraud is the most common crime in England and Wales



14 Office for National Statistics, *UK Population Mid-Year Estimate*, (2024).
15 Office for National Statistics, *Statistics on Crime in England and Wales*, (2025), Volume of CSEW incidents by offence group (Year ending June 2025).
16 HM Inspectorate of Constabulary and Fire & Rescue Services, *Fraud: Time to Choose – An inspection of the police response to fraud*, (2023).
17 Office for National Statistics, *Statistics on Crime in England and Wales*, (2025), table A1, year to June 2025.
18 Home Office and Ipsos, *Economic Crime Survey 2024*, (November 2025), Businesses with employees, paragraph 2.1.

Part One – Disclosure

36. Against this context, I was asked to chair the Independent Review of Disclosure and Fraud Offences. A primary concern, noted in the 2023 Government Fraud Strategy, was that the rise of digital material in criminal investigations has contributed to unacceptable delays for victims and defendants, many of whom have waited years for their day in court. The outdated criminal disclosure regime was identified as a significant cause for this dysfunction. I was asked to evaluate the regime's performance. The Review commenced in October 2023, and I submitted my findings to the Government in November 2024. The final report *Disclosure in the Digital Age* was subsequently presented to Parliament in March 2025.[19]

37. I concluded that a modern disclosure regime is required to prevent the criminal justice system from drowning in a deluge of digital material. Without reform, the State will be rendered impotent in its ability to deliver justice—let alone swift justice. In equal measure, disclosure reform presents an opportunity to make the system more effective and efficient, and to save significant amounts of law enforcement and court time. The Review also found that material heavy cases, such as fraud, were particularly negatively impacted by the current regime.

38. In consultation with a wide range of stakeholders, I proposed a package of reforms to encourage responsible use of advanced technology and artificial intelligence (AI), to assist officers in mastering the mountains of digital material gathered during investigations. I recommended a new Intensive Disclosure Regime pathway for managing disclosure in the most complex and serious cases. I also recommended that higher-quality criminal justice training is required to support law enforcement officers' comprehension of their statutory duties, under the Criminal Procedure and Investigations Act 1996 and accompanying Code of Practice.

39. I remain of the view that modernising the disclosure regime is the single most impactful technical correction the Government can make to improve the journey of a fraud prosecution (as well as other cases heavy in digital files) through the criminal justice system and thereby ensure that cases are resolved efficiently, expediently and efficaciously.

Part Two – Fraud Offences

40. Having completed this first phase, I was asked by the Government to continue the Review, as originally designed, and narrow my focus to the barriers preventing the detection, investigation and prosecution of fraud committed against individuals and businesses. I began Part Two of this Review in March 2025, with the aim of presenting this Report by the end of 2025.

[19] Home Office, *Disclosure in the Digital Age: Independent Review of Disclosure and Fraud Offences*, (2025), CP 1285.

41. The last Independent Review of Fraud, *Report of the Fraud Trials Committee* (the Roskill Report), ran from 1983 to 1986. Unlike that former comprehensive review, conducted over 40 years ago, my examination comes amidst an unprecedented digital transformation. The Roskill Report occurred in an era of paper records and in-person banking. Today's shifting landscape features cryptocurrency, AI and instant global transactions.

42. Criminal methodologies have evolved dramatically, requiring equally sophisticated responses. Digital acceleration during, and after, the COVID pandemic created new vulnerabilities exploited by fraudsters. The very speed at which criminals adopt new fraud techniques presents challenges for both law enforcement and policymakers.

43. Fraud has many guises, and today the most persuasive methods include identity fraud, where personal data is misappropriated to impersonate victims; payment and banking fraud, encompassing credit card and advance fee fraud, account takeover, romance fraud and phishing attacks;[20] and investment fraud, which induces individuals to commit funds to fictitious or grossly misrepresented schemes.

44. Insurance and benefits fraud similarly involve false claims to extract unwarranted payouts, while advance-fee scams and mass-marketing fraud prey on trust and urgency, promising rewards in exchange for upfront payments. Retail fraud is also a substantial threat, involving unlawful tactics like refund scams and price-tag switching. Increasingly, these offences are cyber-enabled,[21] using social engineering techniques to manipulate victims into authorising harmful actions.

Review Aim

45. In light of the substantial and growing threat posed by fraud, I was asked to consult practitioners and identify critical pressure points in the progression of fraud cases through the criminal justice system. Rather than undertaking an exhaustive documentation of the fraud landscape, my aim was to identify timely, actionable recommendations that could deliver meaningful change.

[20] Phishing – An attempt to obtain sensitive information (such as passwords or financial details) by disguising as a trustworthy entity in electronic communications.
[21] Cyber-enabled crime – Traditional offences, such as fraud or theft, that are significantly amplified or facilitated using digital technology and the internet.

Scope and Structure

46. As set out in the Terms of Reference,[22] the Review focused specifically on fraud committed against individuals and businesses, excluding public sector fraud. This Report addresses barriers arising at the following stages within a fraud case lifecycle:

a. **Reporting and Detection** – The means and methods by which law enforcement agencies can detect and disrupt fraudulent activities. This included evaluating incentives for informants within criminal fraud networks, and corporate whistleblowers.

b. **Investigation** – The skills, tools and powers required for investigators to rapidly pursue leads, review case material, and share relevant data with private partners and other law enforcement agencies, including internationally.

c. **Prosecution and Offences** – Evaluating whether fraud offences and the Fraud Act 2006 can keep pace with modern offending. Assessing enablers of fraud such as identity theft, abuse of Deed Poll and the use of AI. Considering whether there should be a greater role for civil penalties.

d. **Courts** – Assessing whether criminal courts are equipped to hear serious or complex fraud cases.

e. **Penalties** – Whether the current penalties fit the crime. Looking beyond custodial sentences, the review considered if courts should be able to use more creative punitive measures. This included evaluating penalties for companies failing in their duties to reduce and prevent fraud.

f. **Rehabilitation** – Considering whether the current network of support for victims is sufficient and what more can be done to rehabilitate offenders.

Methodology

47. Wishing to continue the success of Part One of this Review, a similar evidence-gathering strategy was employed. First, the lifecycle of a fraud case was broken down into its constituent stages, each then examined and analysed. In parallel, the Review identified and interviewed those with first-hand experience investigating, prosecuting, defending and hearing fraud cases. Furthermore, the Review spoke with convicted individuals, victims, and rights groups. Again, I am very grateful to the Bar Council and Law Society, who convened committee meetings in order for the Review to hear views from their members. As with Part One, this consultation was wide ranging. Annex C provides a summary of engagement.

[22] Home Office, *Independent Review of Disclosure and Fraud Offences - Part Two: terms of reference*, (2025).

48. Unlike the disclosure regime, for which there is limited useful quantitative data, greater weight was placed on the use of the analysis of criminal justice system data. However, one limitation of this data is the inability to disaggregate and analyse serious or complex fraud cases, from 'average' fraud cases. This limitation arises from the fact that fraud offences are typically prosecuted under the Fraud Act 2006, which does not differentiate between types or degrees of fraud based on their seriousness. As a result, it is not possible to delineate offences by category or severity using charge data alone. To gain insight into the relative seriousness of fraud cases, analysts have instead relied on proxy indicators, such as the length of final custodial sentences imposed.

Beyond the Balance Sheet

49. In conducting this assessment, I remained acutely aware of the often unseen and deeply personal harm inflicted upon victims of fraud. Beyond the immediate financial loss, victims frequently suffer a profound erosion of trust, and in certain cases, the breakdown of livelihoods due to business collapse. The broader economic consequences of fraud are equally significant, undermining market stability and public confidence in the ability of the State to bring criminals to justice. It is essential to dispel the notion that fraud is a victimless crime. The chief aim of this Review, to identify systemic barriers and propose reforms, is to ensure that both fraud victims and defendants receive swift, fair justice.

2. A Short History of Fraud

Introduction

50. Before addressing the contemporary challenges that fraud presents, it is instructive to glance back at its origins and evolution. Patterns of deception have shadowed human enterprise for centuries, shaping law, commerce and morality. What began as tolerated sharp practice gradually came to be recognised, first as a civil wrong and, ultimately, as a serious criminal offence. This historical trajectory, punctuated by landmark cases and legislative milestones, provides essential context for understanding the framework within which modern fraud is dealt with.

51. Fraud is not a modern invention, but a phenomenon as old as human society itself. Wherever trust has existed, so too has the potential for deception. It is not without significance that the Bible contains a strong prohibition against deceptive conduct, exemplified by the requirement that a person must have 'accurate scales, accurate weights, and an accurate liquid measure',[23] so as to ensure there is no injustice in business dealings.

52. Centuries later, the concept was formalised in language: the Latin term *fraus*, meaning deceit or trickery, appears in classical literature as early as 29 BCE in Virgil's *Aeneid*, where it conveys emotional and moral betrayal.[24] Although the word itself emerged in Roman literary and legal contexts, the behaviours it describes long predate its linguistic codification.

53. Since antiquity, the understanding of what qualifies as fraud has evolved. Even domestically, the last 300 years saw fraud shift from being viewed primarily as a civil misdemeanour to being understood as a criminal offence. In this Review, I have limited my reflections to the period from the 18th century onward, a crucial starting point in understanding the development of the British State and commerce.

18th Century

54. In the 1700s, fraud was seen less as a crime and more as a failure of prudence. The common law favoured the shrewd over the naïve, offering little protection to those who failed to guard against deception. Only when fraud inflicted public harm, particularly against officials, did it rise to the level of felony. Otherwise, it was treated as a civil matter, rooted in misrepresentation and personal risk.[25]

---

[23] Leviticus 19:35–36, circa 1440–1400 BCE.

[24] Virgil (29–19 BCE). *Aeneid*, Book IV, line 675. In: Lewis, C. T, and Short, C. (1879).

[25] Griffith, C.C., *Prosecuting Fraud in the Metropolis, 1760-1820*, (2017).

55. The South Sea Bubble collapse of 1720 exposed the limits of civil fraud enforcement. Misleading claims about trade in slaves and goods fuelled a frenzy of speculation, drawing in nearly 200 companies. When the bubble burst, it triggered widespread financial ruin and shattered public confidence in corporate and government institutions.[26]

56. The scandal exposed the fragility of a new economic model, joint-stock companies,[27] where fragmented ownership allowed directors to prioritise personal gain over shareholder interests.[28] Parliamentary inquiry revealed high-level corruption and insider trading,[29] [30] which resulted in the imprisonment of the Chancellor of the Exchequer, John Aislabie, in the Tower of London.[31] Though justice was delivered through civil and parliamentary proceedings, the episode sparked calls to treat commercial fraud as a matter of public criminal law.[32]

57. The South Sea Bubble resulted in civil penalties rather than criminal prosecutions because investors were widely regarded as the authors of their own misfortune, "wild gamblers gripped by a mania for quick gains", and thus undeserving of legal protection.[33] This view reflected an 18th-century legal culture that placed the burden of risk on the individual.

58. In *R. v Pinkney* (1733), the King's Bench treated selling corn short of measure as a private breach of contract rather than a public cheat, and thus not indictable at common law. This reflected the prevailing view that frauds in ordinary commerce were primarily matters for civil redress.[34]

59. This emphasis on personal responsibility endured in the Victorian *caveat emptor* tradition:[35] buyers bore the burden of inspecting goods; obvious flaws need not be disclosed. At common law, cheating was indictable only if it affected the public or involved false tokens; private cheats were left to civil remedies.

60. Parliament, however, began legislating to recognise the criminal nature of such practices. The Obtaining Money by False Pretences Act 1757[36] criminalised obtaining money or

---

[26] Temin, P. and Voth, H.-J., *Prometheus Shackled: Goldsmith Banks and England's Financial Revolution after 1700*, (2013), chapter 5.
[27] Joint-stock companies – Commercial enterprises in which ownership is divided among shareholders.
[28] Harris, R., 'The Bubble Act: Its Passage and Its Effects on Business Organization', *The Journal of Economic History*, vol. 54, no. 3, 1994, pp. 610–27.
[29] Carswell, J., *The South Sea Bubble*, London: The Cresset Press, (1960), pp. 215–220.
[30] Dickson, P.G.M., The Financial Revolution in England: A Study in the Development of Public Credit 1688–1756, (1967), pp. 312–318.
[31] Parliamentary Archives, *Report of the Trustees in whom the estates of the late South Sea directors and of John Aislabie Esq. are vested*, Presented to the House of Commons, 6 February 1721.
[32] House of Lords, *The Case of the Right Honourable John Aislabie, Esq; Late Chancellor of the Exchequer*, in April 1721, upon the Bill for Inflicting Pains and Penalties on the South-Sea Directors.
[33] Taylor, J., Boardroom Scandal: The Criminalization of Company Fraud in Nineteenth-Century Britain, (2013), page 11.
[34] *R v Pinkney*, 25 e.r. 593; (1733) cited in C. Griffiths, (2017).
[35] Caveat emptor – 'let the buyer beware'.
[36] Obtaining Money by False Pretences, etc. Act 1757 (30 Geo II c 24).

goods "by false pretence or pretences", expressly to protect "industrious families" and the public's "trade and credit".

61. Notwithstanding this change, in *R v Wheatley* (1761), the King's Bench held that selling beer short of the agreed measure was a mere civil breach, not indictable, demarcating the boundary between criminal cheating and contractual wrongs.[37] In civil law, the doctrine of *caveat emptor* predominated: vendors had no general duty to volunteer defects, absent warranty, misrepresentation or active concealment.

62. This principle was clearly illustrated in *Horsfall v Thomas* (1862), where a buyer purchased a defective cannon without inspection.[38] The court held the seller blameless, there was no concealment and therefore no fraud. The court took the view that a fraud would have required either a knowingly false assertion or suppression of a material truth where disclosure is owed.[39]

63. Though *caveat emptor* still ruled the day, the following decades would see a growing appreciation that fraud may constitute more than sharp business practice. In *Redgrave v Hurd* (1881), the Court of Appeal ruled that it was no defence to say the representee could have checked the truth but did not.[40] The defendant must prove the complainant knew the facts, not merely that he had the means to verify them.

19th Century

64. Well into the 19th century, small-scale fraud was still treated primarily as a civil dispute. Yet, as the century advanced, fraud came to be seen less as sharp practice and more as conduct warranting criminal sanction.[41] The rapid expansion of railways in the 1840s exposed the scale of corporate deception. Directors falsified accounts to attract capital, concealing the true financial state of their ventures. Such practices eroded public confidence and intensified calls for criminal liability for those in positions of trust.[42]

65. Confidence collapsed further with the Tipperary Bank scandal of 1856. John Sadleir MP, a prominent financier and politician, had drained the bank through an overdraft of nearly £288,000, using the funds for reckless speculation.[43] To conceal his losses, he resorted to forging deeds, selling fictitious railway shares, and misappropriating rents and client funds, ultimately dissipating over £1 million. When the fraud unravelled, Sadleir fled to

---

37 *R v Wheatley* (1761) 2 Burr 1125; 97 ER 746.
38 *Horsfall v Thomas* (1862) 1 H & C 90.
39 Ibid, at 92.
40 *Redgrave v Hurd* (1881) 20 Ch D 1.
41 Taylor, J., Boardroom Scandal: The Criminalization of Company Fraud in Nineteenth-Century Britain, (2013), page 61.
42 Ibid, page 61.
43 O'Brien, J.B., 'Sadleir's Bank (The Tipperary Joint Stock Bank 1838–56)', *Journal of the Cork Historical and Archaeological Society*, vol. 85, no. 235, 1977, pp. 33–38.

Hampstead Heath and took his own life. The collapse ruined depositors, which are reported to have included small farmers and shopkeepers.[44]

66. The scandals underscored a growing recognition that fraud by directors and public figures posed systemic risks. Legislative reform followed in the mid-late 19th century, with key measures including:

a. **The Joint Stock Companies Act 1844** – Introduced company registration, enhancing transparency.

b. **The Limited Liability Act 1855** – Capped shareholder exposure, encouraging wider investment.

c. **The Companies Act 1862** – Consolidated governance rules and extended limited liability to banks in 1879.

d. **The Sale of Goods Act 1893** – Codified principles requiring goods to match their description, strengthening protection against misrepresentation.

67. Simultaneously, a more fundamental change was taking place. In 1845, the Criminal Law Commission criticised private prosecutions as costly and inconsistent, urging a public agency to assume responsibility.[45] [46] Over 30 years later, the Prosecution of Offences Act 1879 established the role of Director of Public Prosecutions, paving the way for the Crown Prosecution Service in 1986.[47] This marked a decisive shift from private redress to State-led enforcement.

68. By the close of the 19th century, fraud was no longer viewed as a mere civil wrong but as conduct capable of inflicting serious public harm. Legislative and institutional reforms laid the foundation for modern criminal enforcement and statutory protection for victims.

20th Century

69. Building on 19th century reform, the early 20th century saw increased scrutiny of companies and a greater emphasis on consumer protections. The Companies Act 1900 introduced mandatory disclosure requirements for company prospectuses and imposed liability on directors for misstatements.[48] It also introduced stricter auditing requirements and strengthened the Board of Trade's supervisory role.

[44] Ibid.
[45] HM Stationery Office, *Eighth Report of the Commissioners on the Criminal Law*, Criminal Law Commission, (1845).
[46] Royal Commission on Revising and Consolidating the Criminal Law (1845) in Reports from the Royal Commission on the Criminal Law: with appendices and index, 1843–45, (1971).
[47] Prosecution of Offences Act 1985.
[48] Companies Act 1900, s.10.

70. Banking consolidation followed, accompanied by internal controls and a shift towards "impersonal and prudent lending".[49] Technological developments, particularly the widespread adoption of cheques in place of bills of exchange, enhanced the detection and prevention of forgery.[50]

71. Yet controversy persisted. The Marconi scandal of 1912 stands out: senior ministers, including the Chancellor of the Exchequer, were accused of insider trading after acquiring shares in the American Marconi Company shortly before it secured a lucrative government contract.[51] Although the matter was ultimately resolved politically rather than judicially, the affair raised enduring concerns about political integrity, the influence of private interests in public affairs, and the absence of accountability for economic misconduct.

72. Black markets in both World Wars created new opportunities to commit procurement fraud and the forgery of ration books and food tokens.[52] The interwar years, marked by a rising credit-to-GDP ratio,[53] fuelled aggressive competition in lending—creating what commentators described as "a favourable atmosphere for the fraudulent operations of sharks and swindlers".[54]

73. Post-war regulation tightened. The Bretton Woods system of the 1940s imposed fixed exchange rates and capital controls, restricting speculative banking and international flows.[55] In the 1950s, Britain reinforced these constraints through domestic financial repression, tight credit controls, prioritisation of industrial lending, and restrictions on securities markets. These measures shifted growth towards manufacturing and away from speculative finance. By 1970, *The Economist* concluded: "The Wild West days of the City are long past. Hardly any massive swindles, frauds, hoaxes, or gigantic market riggings enliven the scene."[56]

74. The Heath Government continued pursuing a regulatory approach by establishing the Office of Fair Trading (OFT), under the Fair Trading Act 1973,[57] which promoted

---

[49] Roms, S. and Lin, C., '[Economic freedom, financial development and the determinants of fraud and scandal: The United Kingdom 1900–2010]', *Business History*, vol. 67, no. 1, 2023, page 282.

[50] Hollow, M., *Rogue Banking: A History of Financial Fraud in Interwar Britain*, Palgrave Macmillan, (2015).

[51] The National Library of Wales, *The Marconi Scandal*, in David Lloyd George Digital Exhibition, [Accessed 19 September 2025].

[52] Roodhouse, T., *Black Market Britain: 1939–1955*, (2013), chapters 3 and 4.

[53] Gross domestic product (GDP) is a measure of the size and health of a country's economy over time [Source: Bank of England].

[54] Roms, S. and Lin, C., 'Economic freedom, financial development and the determinants of fraud and scandal: The United Kingdom 1900–2010', *Business History*, vol. 67, no. 1, 2025, page 282.

[55] Ibid, page 283.

[56] *The Economist*, 'City City bang bang: The Square Kilometre: A Survey', 8 August 1970, vol. 236, page 63.

[57] Fair Trading Act 1973, s.1.

consumer protection. The OFT was explicitly tasked with safeguarding consumers from "fraudulent, misleading, and anti-competitive business practices".[58]

1980s: Capitalism and the Financial Markets

75. The regulatory zeal of the 1970s ended abruptly with the Thatcher Government's arrival in 1979. Determined to liberalise the economy, it dismantled controls and championed financial freedom, fertile ground for fraud. Credit expanded rapidly, fuelled by the Bank of England's Competition and Credit Control reforms, the collapse of Bretton Woods, and the rise of offshore Eurocurrency markets. Exchange controls were swept away by the General Exemption Order of 13 December 1979,[59] enabling capital to flow abroad with ease. Such activity was facilitated by the rise of tax havens, in Crown Dependencies, and opaque shell companies.

Fraud Trials Committee

76. Predictably, fraud scandals followed, prompting calls for reform. In response, the Lord Chancellor and Home Secretary announced in November 1983 the creation of an independent inquiry, the Fraud Trials Committee, chaired by Lord Roskill. Its remit was clear yet ambitious: to examine how criminal proceedings in England and Wales arising from fraud could be improved, and to recommend changes in law and procedure to ensure trials were just, expeditious and economical.[60] The Committee's scope extended beyond mere trial mechanics; it scrutinised investigation, preparation, and the role of juries in complex fraud cases. Its work culminated in the Roskill Report (1986),[61] a damning indictment of a system ill-equipped to tackle serious fraud.

77. The then Lord Chancellor, Lord Hailsham of Saint Marylebone, captured the mood: "In the United Kingdom, fraud is a growth industry … The public no longer believes that the legal system … is capable of bringing the perpetrators of serious frauds expeditiously and effectively to book. The largest and most cleverly executed crimes escape unpunished."[62]

78. The recommendations of the Roskill Report marked a turning point in the investigation and prosecution of serious fraud. Acting on its proposals, the Government introduced the Criminal Justice Act 1987, which established the Serious Fraud Office (SFO). Uniquely, the SFO was designed to combine both investigative and prosecutorial functions within a single agency, departing from the traditional model in which police or

[58] The Office of Fair Trading was replaced in 2014 with the Competition and Markets Authority.
[59] Companies (Particulars of Usual Residential Address) Regulations 1979, SI 1979/1660.
[60] Levi, M., 'Reforming the Criminal Fraud Trial: An Overview of the Roskill Proposals', *Journal of Law and Society*, vol. 13, no. 1, 1986, page 117.
[61] HM Stationery Office, *Fraud Trials Committee Report*, (1986), Cm 262.
[62] UK Parliament, 'Fraud Trials Committee Report', HL, 10 February 1986, vol. 471 cc. 7–73, [Accessed 20 August 2025].

regulatory bodies investigated offences before passing cases to a separate prosecuting authority.

79. Subsequent Governments continued to draw upon findings from Independent Reviews to inform their fraud policy thinking. The Dearing Report of 1988 led to the establishment of the Financial Reporting Council, which created an independent regulator for auditors, accountants and actuaries, and provided corporate governance and stewardship codes.[63] The 1992 Cadbury Report laid the foundation for a Corporate Governance Code and strengthened the Financial Report Council, which oversaw the Corporate Governance Code.[64] The Hampel Report (1998) followed, reviewing and consolidating earlier recommendations into the Combined Code, emphasising principles-based governance and accountability.[65]

80. During this period, the private sector responded by creating Cifas in 1988. Founded by the Consumer Credit Trade Association with backing from the Office of Fair Trading, Cifas became the UK's first not-for-profit fraud data-sharing scheme, an early public–private partnership enabling real-time exchange of fraud risk intelligence. Today, it remains the largest cross-sector fraud database. The public sector followed with the National Fraud Initiative, piloted in 1993 and fully operational by 1996.[66]

Developing Conception of Dishonesty

81. In parallel to the regulatory reform of the 1900s, the legal conception of dishonesty also evolved, but there remained a lack of clarity regarding the agreed definition of 'fraudulent' behaviour. This central issue was tackled by the 1966 Criminal Law Revision Committee, who called for a change in language from 'fraudulent' to 'dishonesty'.[67] Dishonesty subsequently became a core component of the Theft Acts of 1968 and 1978.

82. In adopting this revision, a central question emerged: how should dishonesty be defined? This was considered by Lord Roskill, who observed that there was no statutory definition of dishonesty. He noted that an entirely objective test risked convicting individuals who lacked genuine moral culpability, while a purely subjective approach would allow defendants to set their own standards of honesty, undermining the consistency and integrity of the law. Without a statutory definition, the law risked inconsistency, particularly given differing views among ordinary people as to what constitutes dishonest

[63] Department of Trade and Industry, The Making of Accounting Standards: Report of the Review Committee Under the Chairmanship of Sir Ronald Dearing: a Consultative Document from the Department of Trade and Industry, (1989).
[64] The Committee on the Financial Aspects of Corporate Governance, *The Financial Aspects of Corporate Governance*, (1992).
[65] Committee on Corporate Governance, *Final Report* (Hampel Report), (1998).
[66] Cabinet Office, *National Fraud Initiative Report*, (2020).
[67] HM Stationery Office, Eighth Report, Criminal Law Revision Committee: Theft and Related Offences, Cm 2977, (1966).

behaviour. This conundrum would be dealt with head on by the Court of Appeal, in *R v Ghosh* (1982).[68]

R v Ghosh (1982)

83. The case involved a hospital locum consultant, Deb Ghosh, who falsely claimed payment for a surgical procedure he had not performed. Ghosh was subsequently charged under sections 15(1) and 20(2) of the Theft Act 1968 for obtaining money by deception. The central issue in the case was the legal definition of 'dishonesty'. The Court of Appeal, led by Lord Lane CJ, upheld the conviction and established a two-limb test:[69]

a. **An objective test** – Examining whether, according to the ordinary standards of reasonable and honest people, the action in question was dishonest.

b. **A subjective test** – Examining whether the defendant realised that their conduct was, by those standards, dishonest.

Cyber-Enabled Fraud Emerges

84. As fraud evolved, so did its instruments. The technological revolution transformed the landscape. The first electronic digital computer, ENIAC, appeared in 1945,[70] but for decades computers were the preserve of corporations, universities and hobbyists. By the 1980s, falling costs and rising demand brought them into homes, creating new opportunities for crime, alongside convenience.

85. The Government saw the potential early. Margaret Thatcher, then Prime Minister, launched a scheme to subsidise school computers, declaring that Britain's prosperity depended on children mastering this new technology. Her words were prescient: "Our future prosperity depends in large part on the quality of education today… children should also be able to understand computers and how they can be used and applied."[71]

86. The modern internet followed. In 1983, computers began to connect and talk to each other, unlocking innovation, and exposing fresh vulnerabilities. Connectivity became the gateway for emerging forms of fraud, committed by criminals exploiting digital networks.

87. By 1985, 12% of British households owned a computer.[72] Optimism soon collided with legal uncertainty. In *R v Schifreen* (1988), two hackers used home computers and modems to infiltrate British Telecom's Prestel service—including Prince Philip's inbox.

---

[68] *R v Ghosh* [1982] QB 1053.
[69] Ibid.
[70] Encyclopaedia Britannica, 'ENIAC: computer', [Accessed 29 October 2025].
[71] Margaret Thatcher Foundation, 'Speech on microcomputers in schools', (1981), [Accessed 19 September 2025].
[72] Office for National Statistics, *Percentage of households with durable goods: 1970 to financial year ending 2018*, (2019), [Accessed 19 September 2025].

Prosecutors reached for the Forgery and Counterfeiting Act 1981, but the convictions collapsed on appeal. The House of Lords ruled that, while unethical, the conduct was not criminal.[73]

88. In their subsequent report, the Law Commission stressed the need for new legislation which criminalised unauthorised access and the misuse of computer systems.[74] This led to the enactment of the Computer Misuse Act 1990 and offences thereunder.[75]

R v Preddy (1996)

89. As the millennium neared, cracks in the State's armour against fraud were laid bare, none starker than in R *v Preddy and Slade* (1996). The defendants secured property loans through false representations, triggering transfers from mortgage lenders to their accounts. A jury convicted under section 15(1) of the Theft Act 1968: obtaining property by deception.

90. The Court of Appeal upheld the verdict but certified questions of law. However, following a successful appeal to the House of Lords, all convictions were quashed. The House of Lords found that, because the mortgage lenders' accounts did not show a corresponding decrease and the credit balances created were new, the property obtained did not 'belong to another', as required by section 15. As a result, the conduct fell outside the scope of the Theft Act 1968.[76] In response, the Theft Act 1968 was revised by the Theft Act 1978, which created several additional criminal offences. However, this did not resolve the underlying issue and instead led to a problem of offences being overly specific.

21st Century

91. The new millennium marked a decisive turning point in the nature of criminal activity. The proliferation of internet-connected devices and digital tools enabled individuals, whether acting alone or as part of serious and organised criminal networks, to exploit technology for fraudulent purposes with unprecedented reach, speed and anonymity. This ushered in a new era in which cyber-enabled and online fraud rapidly became dominant, challenging traditional enforcement models and exposing the limitations of existing legal frameworks.

92. In response, Parliament enacted a series of legislative and regulatory reforms. Chief among these was the Proceeds of Crime Act 2002 (POCA),[77] which provided law enforcement agencies with a comprehensive framework for the recovery of criminal assets. POCA addressed both domestic and international criminal conduct, including money laundering, and introduced confiscation orders post-conviction in the Crown

---

[73] R v Gold and Schifreen [1988] 2 WLR 984.
[74] Law Commission, *Computer Misuse: Report on Criminal Law Reform,* (1989), Law Com No 186, Cm 819.
[75] See chapter 'Legislative Landscape'.
[76] R v Preddy and Slade [1996] UKHL 13.
[77] Home Office, *Serious Crime Bill – Fact sheet: Overview of Proceeds of Crime Act 2002*, (2014), [Accessed 19 September 2025].

Court. Crucially, it also allowed for civil recovery proceedings in the High Court without the need for a criminal conviction, an innovation that recognised the evidential challenges posed by complex financial crime.

93. Part 7 of POCA imposed reporting obligations on regulated sectors, notably financial institutions, to prevent money laundering and improve intelligence flows. The Act also established the Asset Recovery Agency (ARA), which was granted powers to pursue civil recovery and use taxation measures to reclaim criminal income where there was reasonable suspicion.

94. However, the ARA proved short-lived. By December 2006, it had recovered only £23 million in assets against an expenditure of £65 million.[78] The National Audit Office concluded that the agency was not delivering value for money,[79] and in 2007 its functions were merged into the newly formed Serious Organised Crime Agency (SOCA), which itself would later be subsumed into the National Crime Agency (NCA).[80] [81]

95. Alongside POCA, the creation of the Financial Services Authority (FSA) in 2000 signalled a moderate shift towards greater oversight of financial markets. This institutional reform was a response to growing concerns about market integrity and the adequacy of regulatory supervision in an increasingly globalised financial system.

Law Commission Report 2002

96. The inadequacy of existing fraud legislation became increasingly apparent in the early 1990s, as a series of high-profile cases, such as *R v. Marcus & Others* and the Maxwell Pension Scandal, collapsed due to what was perceived to be technical deficiencies in the law.[82] These cases exposed the limitations of deception-based offences under the Theft Acts. In response, the then Home Secretary, Jack Straw, asked the Law Commission to undertake a comprehensive review of fraud offences.[83] The resulting report, published in 2002, was a landmark moment in the modernisation of fraud law.[84]

97. The Commission identified two principal flaws in the legal framework, which was governed by the Theft Acts of 1968 and 1978. First, the offences were overly technical and difficult to apply consistently, particularly in cases involving digital transactions. Second, they required that any deception be 'operative', meaning it must cause the victim to act in a way that leads to the transfer of property, a requirement that proved

78 House of Commons Committee of Public Accounts, *Assets Recovery Agency*, (2007), HC 391, page 3.
79 National Audit Office, *The Assets Recovery Agency*, (2007), HC 253.
80 BBC News, 'Assets Recovery Agency Abolished', 11 January 2007, [Accessed 19 September 2025].
81 Crime and Courts Act 2013, s. 15(1).
82 *R v. Marcus & Others* (Blue Arrow Case) [1992] and *R v. Kevin Maxwell & Others* (Maxwell Pension Scandal).
83 Dyer, C., 'Fraud laws need to be simplified, says commission', *The Guardian*, 30 July 2002, [Accessed 19 September 2025].
84 Law Commission, *Fraud: Report on a reference under section 3(1)(e) of the Law Commissions Act 1965*, (2002), Cm 5560, pp. 16–17.

problematic in complex financial arrangements, as illustrated in the case of *R v Preddy*, where the legal fiction of property transfer rendered the offence inapplicable.[85]

98. The Commission recommended the creation of a single, general offence of fraud, capable of adapting to evolving methods of deception. This proposal was designed to simplify the law, improve prosecutorial clarity, and ensure that emerging forms of fraud, particularly those involving electronic communications, could be effectively addressed.

99. Following the Commission's report, the Government launched a public consultation in 2004 titled *Fraud Law Reform*, which broadly endorsed the recommendations.[86] A Fraud Bill was subsequently introduced in Parliament in May 2005 and received cross-party support. The resulting Fraud Act 2006 implemented the Commission's proposals, establishing a general offence of fraud and codifying three principal methods: fraud by false representation, fraud by failing to disclose information, and fraud by abuse of position.[87] This Act remains the cornerstone of fraud prosecution in England, Wales and Northern Ireland.

Attorney General's Fraud Review 2006

100. Published in 2006, the Attorney General's Fraud Review was the first comprehensive assessment of fraud across both public and private sectors.[88] It responded to growing concern over the complexity of fraud and the inadequacy of existing systems. The Review found fraud to be widespread, under-reported, and often linked to serious organised crime. Victims frequently chose not to report offences due to shame or distrust in law enforcement, creating a cycle of silence and under-prioritisation. It highlighted fragmented enforcement, poor data collection, and the absence of a coherent national strategy.

101. To address these failings, the Review proposed the creation of a National Fraud Strategic Authority (NFSA) to lead public education, prevention and enforcement.[89] It called for improved data-sharing between agencies and the establishment of a dedicated financial court to hear both civil and criminal fraud cases.[90] Crucially, it endorsed the Fraud Bill then progressing through Parliament, reinforcing the need for a simplified and flexible legal framework. The Review concluded that a coordinated national strategy was vital if the Government were to seriously tackle the scale and sophistication of the threat.

85 Jiaqi, L., 'Critically Analysis of the Fraud Act 2006', *Academic Journal of Management and Social Studies*, vol. 5, no. 2, 2023, pp. 8–10.
86 UK Parliament, 'Fraud Law Reform', HC, vol 421, debated on Monday 17 May 2004.
87 Fraud Act 2006.
88 Attorney General's Office, *Fraud Review: Final Report*, (2006).
89 Ibid, page 6.
90 Ibid, pp. 158–159.

The Rise of Social Media

102. While the Fraud Act 2006 modernised the legal framework, this period saw the rapid emergence of social media platforms that fundamentally reshaped the fraud landscape. Early platforms like MySpace, Hi5, and Friendster introduced personal profiles and private messaging, but it was Facebook that transformed global connectivity, growing from one million users in 2004[91] to over a billion by 2012.[92] These platforms enabled political mobilisation and cross-border dialogue but also created fertile ground for deception. The same features that empowered democratic engagement—reach, anonymity and speed—were quickly exploited by fraudsters and bad actors.

103. Social media facilitated a shift from mass fraud to targeted manipulation. Early scams included phishing emails and fake profiles, often tailored to exploit trust-based interactions. Fraudsters used personal data to extract financial information or direct payments, blurring the line between social interaction and criminal enterprise. As digital life became more embedded, fraud became more scalable, personalised, and difficult to detect, ushering in a new phase of economic crime.

104. These platforms dramatically transformed the ways in which people communicate with one another, empowering individuals to connect across borders and enabling political dissidents to organise and share ideas beyond the reach of oppressive regimes. From the Arab Spring to protests in Hong Kong, its democratic potential was clear. Yet the very attributes that fostered openness also created fertile ground for deception, allowing fraudsters to exploit vulnerable individuals at unprecedented scale.

Financial Collapse of 2008

105. The global financial crisis of 2008 marked a watershed moment in the history of economic crime. Triggered by the widespread misrepresentation of risk in mortgage-backed securities, failures in corporate governance and reckless lending practices, the crisis exposed deep structural weaknesses in financial regulation and accountability.

106. In the UK, the impact was severe. GDP fell by over 6% between early 2008 to mid-2009 and unemployment peaked at 8.4%, its highest level since 1995. Over 19,000 companies were forced into liquidation in 2009 alone.[93] Major financial institutions such as Northern Rock and Bradford & Bingley collapsed, while others, including the Royal Bank of Scotland and Lloyds, required unprecedented state intervention. The Government

[91] World Economic Forum, '[How Facebook grew from 0 to 2.3 billion users in 15 years](#)', (2019).
[92] Ortiz-Ospina, E., '[The rise of social media](#)', OurWorldinData.org, (2019), [Accessed 30 October 2025].
[93] Office for National Statistics, *The 2008 recession 10 years on*, (2018), [Accessed 19 September 2025].

injected £137 billion to stabilise the banking sector,[94] prompting widespread public outrage and renewed scrutiny of financial mismanagement and 'white-collar' crime.

107. Yet, despite the scale of misconduct, criminal prosecutions were rare. The crisis laid bare the limitations of existing enforcement mechanisms and the difficulty of attributing individual criminal liability within complex corporate structures. It also revealed a permissive culture in which misrepresentation and concealment were tolerated, if not incentivised, by financial institutions.

108. In response, the Government introduced reforms aimed at strengthening corporate governance and enhancing transparency. These included:

a. The enactment of the Bribery Act 2010, which reinforced the Serious Fraud Office's role as the principal enforcer of anti-bribery laws and introduced corporate liability for failure to prevent bribery.[95]

b. The introduction of Deferred Prosecution Agreements (DPAs) under Schedule 17 of the Crime and Courts Act 2013, allowing prosecutors to hold companies to account for wrongdoing without pursuing full criminal trials.[96]

109. The crisis also catalysed a broader shift in public and political attitudes toward fraud. It underscored the need for a more robust legal and institutional framework capable of addressing systemic dishonesty, not just individual deception. Fraud was no longer seen as a peripheral offence; it had become a central threat to economic stability and public trust.

Action Fraud Launched 2009

110. In the wake of the Attorney General's Fraud Review and the 2008 financial crisis, the Government concluded that the volume of fraud reports was beginning to overwhelm local forces and that there remained a need for a centralised system to better understand and respond to the true scale of fraud.[97] This led to the creation of the National Fraud Authority (NFA) in 2008, which provided strategic oversight. This was followed by the launch of Action Fraud, in 2009, as the UK's national reporting centre for fraud and cybercrime. Working with the National Fraud Intelligence Bureau (NFIB), Action Fraud aimed to break the cycle of under-reporting by triaging cases and passing possible viable leads to local police forces.

---

[94] House of Commons Library, *Bank rescues of 2007-2009: outcomes and cost'*, Briefing Paper no. 5748, 8 October 2018.
[95] Bribery Act 2010.
[96] Serious Fraud Office, 'SFO Deferred Prosecution Agreements', (2025).
[97] Fraud Advisory Panel, *The Fraud Review: ten years on. Review of progress made since the landmark 2006 UK Fraud Review*, (2016), page 2.

111. Significant improvements in outcomes were not forthcoming, so in 2014, under then Home Secretary Theresa May MP, the NFA was dissolved and its functions redistributed: strategic oversight moved to the NCA; Action Fraud and NFIB came under the City of London Police; and fraud awareness campaigns were handed to the Home Office.[98] The Cabinet Office remained strategically responsible for countering fraud committed against the State. Despite these reforms, concerns persisted about effectiveness, resourcing, and whether fraud was truly prioritised within law enforcement.

2010s

112. The decade following the global financial crisis offered no reprieve from the intensifying scrutiny of economic crime. Far from abating, public and political concern deepened, culminating in the prosecution of several traders for conspiring to manipulate benchmark interest rates such as LIBOR and Euribor, an apparent breakthrough in the fight against market abuse. These convictions were heralded as a clear signal that financial misconduct would no longer be met with impunity.[99]

113. However, the UK Supreme Court later overturned key convictions,[100] ruling that juries had been misdirected in assuming trading advantage equated to dishonesty. The judgment clarified that dishonesty must be judged by the standards of reasonable people, not presumed from motive.[101] The judgment exposed the difficulty of prosecuting fraud in opaque financial environments and further tethered the legal understanding of dishonesty to the objective standards of commercial reasonableness, reaffirming that contractual and financial conduct must be assessed not by the actor's subjective belief but by reference to what a reasonable person would consider honest in the context of prevailing market norms.

Patisserie Valerie Collapse

114. In 2018, the collapse of Patisserie Valerie revealed a £94 million accounting fraud that impacted the UK high street. The company, with over 170 stores and 2,700 employees, had falsified its accounts and misled investors and regulators. Subsequently, the bakery's administrators filed a £200 million lawsuit against their financial auditors, Grant Thornton, for failing to detect the fraud. An out-of-court settlement was reached, with the financial terms not disclosed.[102] The case highlighted the fragility of corporate governance and reinforced calls for reform in audit oversight and accountability.[103]

[98] Home Office, 'National Fraud Authority', written statement to Parliament, 2 December 2013, [Accessed 19 September 2025].
[99] *R v Hayes* [2015] EWCA Crim 1944 and *R v Palombo* [2024] EWCA Crim 304.
[100] R (Respondent) v Hayes (Appellant); R (Respondent) v Palombo (Appellant) [2025] UKSC 29 (appeal from [2024] EWCA Crim 304).
[101] Ticehurst, B., 'Tom Hayes' Libor-rigging conviction quashed by the Supreme *[sic]* Court', *Financial Times Adviser*, 31 July 2025, [Accessed 22 September 2025].
[102] Kate Beioley, 'Patisserie Valerie settles with Grant Thornton over £200mn claim', *Financial Times*, 26 June 2022.
[103] Dan Bryne, *What was the Patisserie Valerie controversy?*, (2018), Corporate Governance Institute.

Post Office Horizon Scandal

115. The Horizon scandal, which gained national attention in the 2010s, saw hundreds of sub-postmasters wrongly prosecuted for fraud and theft due to faulty accounting software.[104] Many lost their livelihoods, reputations and, in some cases, their liberty. Worse still, it has been reported that at least 13 people may have taken their own lives as a result of the immense stress and false accusations they faced. After significant campaigning, the event is now recognised as one of the UK's worst miscarriages of justice. It raised urgent questions about the disclosure of exculpatory material and the treatment of whistleblowers. To date, over £1.2 billion in redress has since been paid to victims.[105]

Evaluation of Legislation

116. In 2012, the Ministry of Justice reviewed the Fraud Act 2006 and found it to be effective, flexible and well-suited to modern fraud.[106] Law enforcement praised its clarity and ability to respond quickly to emerging threats without requiring new offences.[107] The review also reaffirmed the value of the common law offence of conspiracy to defraud, especially in complex cases involving multiple actors. It concluded that the offence remained "essential" and "allowed the totality of the criminal enterprise to be captured in one short count which enabled the court to see the whole picture".[108]

Social Media Society

117. Social media continued to mature through the 2010s, with platforms increasingly shifting focus toward visual and video-based content. This evolution transformed user engagement, with platforms like X (formerly Twitter) reporting that over 50% of viewed content included images or videos.[109] The rise of smartphones and faster internet access further accelerated this trend, making multimedia sharing central to the social media experience.

118. The decade also saw the emergence of new-generation platforms such as TikTok, launched in 2016, which reached 500 million users by mid-2018.[110] These platforms prioritised short-form video and algorithm-driven content discovery, reshaping how users consumed and interacted with media. Thus, the rise in social media providers created new hunting grounds for fraudsters to meet and interact with potential victims.

---

104 BBC News, *Post Office Horizon scandal: Why hundreds were wrongly prosecuted*, updated 9 October 2025.

105 Department for Business and Trade, *Post Office Horizon financial redress data as of 30 September 2025*, (2025), [Accessed 12 December 2025].

106 Ministry of Justice, Post-Legislative Assessment of the Fraud Act 2006: Memorandum to the Justice Select Committee, (2012), Cm 8372.

107 Ibid, page 6.

108 Ministry of Justice, *Post-Legislative Assessment of the Fraud Act 2006,* (2022), CP 680, pp. 17–18.

109 Ortiz-Ospina, E., 'The rise of social media', OurWorldinData.org, (2019), [Accessed 22 September 2025].

110 Ibid.

Recording Fraud

119. In 2015, the Government took steps to reduce its fraud prevalence blind spot. For the first time, fraud was to be included in the Crime Survey for England and Wales (CSEW).[111] Unlike metrics that strongly suffer from under-reporting because they require a victim to make the first move, it was assessed that the telephone sampling model of the CSEW can give a more accurate picture of fraud prevalence.[112]

120. In 2018, the Government launched the National Economic Crime Centre (NECC), housed within the NCA, to improve coordination and intelligence sharing across agencies tackling economic crime.[113] The NECC was designed to be supported by external expertise from the NCA, Serious Fraud Office, Financial Conduct Authority, HM Revenue and Customs, City of London Police and the Crown Prosecution Service, reflecting a more integrated approach to economic crime.

121. This development followed a longer institutional evolution. The National Criminal Intelligence Service (NCIS), established in 1992, was merged into the SOCA in 2006, which itself was replaced by the NCA in 2013. These bodies were created to address organised crime, including money laundering, which remains a key enabler of fraud. The NECC's formation marked a shift toward intelligence-led enforcement, with a particular focus on improving the quality of suspicious activity reporting and enhancing the UK's response to complex, cross-border financial threats.

Ivey v Genting Casinos (2017)

122. Amid growing awareness of fraud's complexity and institutional reform, the legal definition of dishonesty itself came under scrutiny. This culminated in the landmark Supreme Court ruling in *Ivey v Genting Casinos* [2017] UKSC 67, a civil case that reshaped the test for dishonesty in law.[114]

123. Phil Ivey, a professional poker player, sued Genting Casinos after they refused to pay out £7.7 million in winnings, alleging he had cheated using a technique known as 'edge-sorting'. By identifying subtle manufacturing flaws on the backs of playing cards, Ivey gained a significant advantage. He argued that his actions amounted to legitimate gamesmanship and were not dishonest.

124. The case challenged the second limb of the *R v Ghosh* test, which required that the defendant recognise their conduct as dishonest by societal standards. The Supreme Court

[111] Office for Statistics Regulation, *Review of fraud and computer misuse statistics for England and Wales*, (2025), page 11.
[112] CSEW uses interviews to capture victim-based crimes. It generally provides a better measure of trends over time compared with police recorded crime; however, it does not include experiences of sexual assault, stalking and harassment, crimes against society such as drug possession, or crimes against commercial or public sector bodies, tourists and non-household populations.
[113] National Crime Agency, 'National Economic Crime Centre', [Accessed 22 September 2025].
[114] *Ivey v Genting Casinos* (UK) Ltd t/a Crockfords [2017] UKSC 67, [2018] AC 391.

rejected this subjective element, ruling that dishonesty should be judged solely by the objective standards of ordinary decent people.[115] This decision clarified and simplified the legal test, aligning civil and criminal standards and reinforcing the principle that ignorance of societal norms is no defence to fraud.[116]

125. As Lady Hale explained in an extra-judicial lecture following the Supreme Court's judgment in *Ivey v Genting Casinos*: "Although it was not necessary for our decision, and thus strictly *obiter dicta*, we went on to consider the meaning of dishonesty in the criminal law. This was because the law had got itself into a very strange position, such that Mr Ivey could claim that he and Ms Cheung were not dishonest in law, despite having deliberately set out to deceive the croupier into doing something to distort the odds in what was supposed to be a game of pure chance."[117]

126. Although Ivey arose in a civil context, the Court's analysis of criminal dishonesty was expressly *obiter*; nevertheless, it was adopted almost immediately by the criminal courts, within a week, the Divisional Court in *DPP v Patterson*[118] confirmed that the second limb of *Ghosh* no longer applies.

2020s

127. The COVID-19 pandemic triggered a sharp rise in fraud. As lockdowns confined people to their homes and daily life moved online, fraudsters exploited increased isolation and digital reliance. New vulnerabilities emerged in e-commerce, remote working and online banking, while government support schemes were targeted through impersonation and false claims.[119] UK Finance reported that, in 2020, there was a 32% increase in reports of investment scams, a 38% rise in reports of romance fraud, and a 7% increase in purchase scams, compared with the previous year.[120] Fraudsters also sold fake COVID-19 tests and protective equipment, demonstrating how quickly tactics adapt to societal disruption.[121]

Artificial Intelligence

128. The turn of the decade also did not slow the steady march of technological advancement. Early 2020 saw significant advances in artificial intelligence (AI), which began reshaping industries—and criminal tactics. The public release of the large language model ChatGPT in November 2022 further reduced barriers to entry for those willing to try fraud. Criminal groups quickly adapted, developing tools such as FraudGPT, uncensored AI models used

---

[115] Ibid, page 18, para 58.
[116]Ibid, page 27, para 74.
[117] Bristol Alumni Association Lecture, 'Dishonesty, Lady Hale, President of the Supreme Court, 23 February 2018. Referring to *Ivey v Genting Casinos (UK) Ltd t/a Crockfords* [2017] UKSC 67, [2017] 3 WLR 1212.
[118] *DPP v Patterson* [2017] EWHC 2820 (Admin) (Div Ct).
[119] HM Treasury, *Government Action on Fraud in Covid Support Schemes*, (2024), [Accessed 22 September 2025].
[120] UK Finance, *Fraud – The Facts 2021*, [Accessed 22 September 2025].
[121] BBC News, 'Coronavirus tests and masks sold by fraudsters online', 10 April 2020, (video), [Accessed 22 September 2025].

to craft phishing emails, automate scams and build hacking tools.[122] AI also enabled realistic deepfake audio and video, now routinely used in romance scams,[123] investment fraud and identity theft.[124] [125]

129. Simultaneously, the rise of cryptocurrencies[126] introduced new challenges. These decentralised assets bypass traditional banking systems and offer anonymity, making them attractive for fraud and money laundering. The Financial Ombudsman Service report that over half of all investment scams now involve crypto-assets.[127] Reports have noted hostile state actors using cryptocurrencies to evade sanctions and fund illicit activity.[128]

130. In response, industries have begun deploying AI defensively, banks use machine learning to monitor spending patterns and flag suspicious activity, while telecoms providers analyse network traffic to detect SIM swapping and call forwarding fraud.[129] [130] These developments show that, while advanced technology facilitates fraud, it can also be used to fight it.

Increasing Parliamentary Scrutiny

131. In 2022, the Ministry of Justice published a second Post-Legislative Review of the Fraud Act 2006,[131] concluding that the Act continued to meet its original objectives: simplifying fraud law, enabling effective prosecutions and adapting to evolving technologies. Stakeholders, including law enforcement, prosecutors and regulators, agreed that the Act remained fit for purpose, with offences that are clear, flexible, and applicable to a wide range of modern frauds.

132. Despite seemingly sound legislation and growing awareness, fraud remained under-prioritised across government and law enforcement. The House of Lords Committee on Digital Fraud (2022) concluded that a "permissive culture" had taken root, allowing fraud to flourish.[132]

---

122 Ibid.
123 Moseley, S., *Automating Deception: AI's Evolving Role in Romance Fraud*, (2025), Centre for Emerging Technology and Security – The Alan Turing Institute.
124 Lin, L., 'Examining the Role of Deepfake Technology in Organised Fraud: Legal, Security, and Governance Challenges', Frontiers in Law, 4, 2025, pp. 6-17.
125 National Consumers League *Deepfakes, Chatbots, and Scams: How AI is fuelling Fraud and What Policymakers Must Do*, (2025), [Accessed 22 September 2025].
126 Cryptocurrencies – Digital currencies, tokens or assets that use cryptographic techniques to secure transactions, control the creation of new units, and operate on decentralized networks without reliance on a central authority.
127 Office of Financial Sanctions Implementation and HM Treasury, *Cryptoassets: Threat Assessment*, (2025).
128 Ibid.
129 Athens, M., 'AI in Banking Fraud Detection: How does it work?', BankersHub, 17 June 2025, [Accessed 22 September 2025].
130 Bridge Connect, 'How do telecoms use AI for fraud prevention?', 12 March 2025, [Accessed 18 September 2025].
131 Ministry of Justice, Post-Legislative Assessment of the Fraud Act 2006: Memorandum to the House of Lords Select Committee for the Fraud Act and Digital Fraud, (2020), Cm 680.
132 House of Lords, *Fighting Fraud: Breaking the Chain*, (2022), HL Paper 87, page 4.

133. The House of Commons Justice Committee echoed these concerns,[133] citing chronic under-investigation, lack of judicial capacity and the absence of measurable targets. Action Fraud was described as not fit for purpose.[134] These reports called for a comprehensive national strategy, mandatory performance metrics and increased police training. The Treasury Committee also stressed the need to tackle online scam adverts and to introduce regulations against cryptocurrencies.[135]

Economic Crime Plans 2019 and 2023

134. After decades of silence from the Government regarding its strategic plan to tackle financial crime, two Economic Crime Plans were published. The first 2019 Plan[136] was followed by a second in 2022.[137] Together, they set out measures to address economic crime, including reforms to Companies House and the corporate transparency regime, strengthening oversight under the Money Laundering Regulations, and proposals for the new corporate offence of 'failure-to-prevent' fraud. The plans also outlined steps to improve asset recovery, expand law enforcement capability and enhance public–private intelligence sharing.

Government Fraud Strategy 2023

135. Seventeen years after the Attorney General's original recommendation, the Government published a Fraud Strategy[138] committing to a series of reforms. These included the creation of a National Fraud Squad (NFS), comprising 500 specialist posts led by the NECC and City of London Police, and making fraud a strategic policing requirement.

136. In March 2024, the United Kingdom (UK) hosted the inaugural Global Fraud Summit, bringing together partners from across the G7, Five Eyes, Singapore and Republic of Korea, alongside the International Criminal Police Organization (Interpol), UN Office of Drugs and Crime, and the European Commission.[139] In October 2024, the UK secured the first United Nations (UN) resolution on fraud.[140] These actions signalled the Government's intention to take a leading role in tackling transnational fraud.

137. The Government also committed to replacing Action Fraud with a new service 'Report Fraud', aimed at improving victim reporting experience, through an updated website, improved call-handling capacity, and increasing the volume and quality of intelligence packages shared with law enforcement. Time will tell how effective this new service will

---

133 House of Commons Justice Committee, *Fraud and the Justice System*, (2022), HC 12, para 145.
134 Ibid, chapter 2, para 41.
135 House of Commons Treasury Committee, *Economic Crime*, (2022), HC 145, pp. 3–5.
136 Home Office and HM Treasury, *Economic Crime Plan 2019-22*, (2019).
137 Home Office and HM Treasury, *Economic Crime Plan 2023-2026*, (2023).
138 Home Office, *Fraud Strategy: stopping scams and protecting the public*, (2023), CP 839.
139 Home Office, *Global Fraud Summit Communiqué: 11 March 2024*, (2024).
140 United Nations, 'Implementation of the provisions on technical assistance of the United Nations Convention against Transnational Organized Crime', in *Report of the Conference of the Parties to the United Nations Convention against Transnational Organized Crime on its twelfth session, held in Vienna from 14 to 18 October 2024*, (2024), Resolution 12/2, [Accessed 22 September 2025].

be; however, early indications are promising. The new service will also enable victims to track cases progression. The rollout of the Report Fraud service was completed on 4 December 2025, following a phased implementation.

138. In parallel, the Government has continued to collaborate with the private sector through the Joint Fraud Taskforce (JFT), which has developed a series of voluntary sector charters aimed at reducing fraud and improving consumer protection. These include two Telecommunications Fraud Charters,[141] [142] which set out plans to block scam calls and smishing texts,[143] strengthen identity checks, and improve data-sharing across the sector. The JFT has also led the development of the Online Fraud Charter,[144] focused on tackling scam adverts and phishing content on digital platforms, and the Insurance Fraud Charter,[145] which targets ghost broking, illegal intermediaries and data theft.

139. The Government also introduced the Economic Crime (Transparency and Enforcement) Act 2022 and the Economic Crime and Corporate Transparency Act 2023. The 2022 Act established a new Register of Overseas Entities to improve transparency in UK property ownership, strengthened sanctions enforcement and reformed Unexplained Wealth Orders. The 2023 Act includes a new 'failure-to-prevent' fraud offence which holds large organisations criminally liable if a specified fraud offence is committed by an employee or agent for the organisation's benefit, and the organisation failed to have reasonable fraud prevention procedures in place.[146] The Act also expands asset recovery powers under POCA, and includes provisions for freezing and seizing crypto-assets.[147]

Platform Accountability

140. As fraud increasingly intersects with the digital economy, concerns have grown about the role of online platforms in facilitating criminal activity. Recognising the challenge of regulating multi-national technology companies, the UK Government adopted a dual approach: encouraging voluntary action through initiatives such as the Online Fraud Charter, while also pursuing firmer regulation for accountability and public protection.

141. The Online Safety Act 2023 marked a major shift in platform responsibility.[148] It imposed legal duties on digital platforms to prevent and remove harmful content, including fraudulent content. Ofcom was granted enforcement powers to fine non-compliant platforms and require transparency through published risk assessments and mitigation

141 Home Office, *Fraud sector charter: telecommunications*, (2021).
142 Home Office, *UK Telecommunications Fraud Sector Charter*, (2025).
143 Smishing is 'Short Message Service'-based phishing – fraudulent text messages used to steal personal or financial information.
144 Home Office, *Online Fraud Charter*, (2023).
145 Home Office, *Fraud sector charter: insurance*, (2024).
146 Economic Crime (Transparency and Enforcement) Act 2022.
147 Economic Crime and Corporate Transparency Act 2023.
148 Online Safety Act 2023.

strategies. While the Act's long-term impact remains to be seen, its implementation reflects a broader desire for regulation capable of disrupting online criminal behaviour.

Conclusion

142. Through this brief examination of fraud's modern history, a clear trajectory emerges. Fraud has evolved from a moral betrayal and civil dispute into a serious criminal offence rooted in deception, abuse of trust, and the theft of substantial sums from individuals, businesses and the State.

143. Cycles of financial regulation and deregulation have shaped its prevalence, but the advent of the internet marked a decisive shift. It introduced a new era of connectivity, making private technology and communications platforms central to the facilitation of fraud. The rise of AI and cryptocurrencies has further complicated the landscape, enabling new forms of deception and challenging traditional enforcement models.

144. What has remained constant is the human capacity to deceive for gain, and the State's obligation to respond. The legislative reforms, institutional restructurings and strategic initiatives outlined in this chapter reflect an evolving understanding of fraud as a dynamic, systemic threat. They also underscore the need for continued vigilance, innovation and collaboration across sectors. In short, and as discussed in the next chapter, fraud has become the defining crime of our digital age.

3. Contemporary Picture

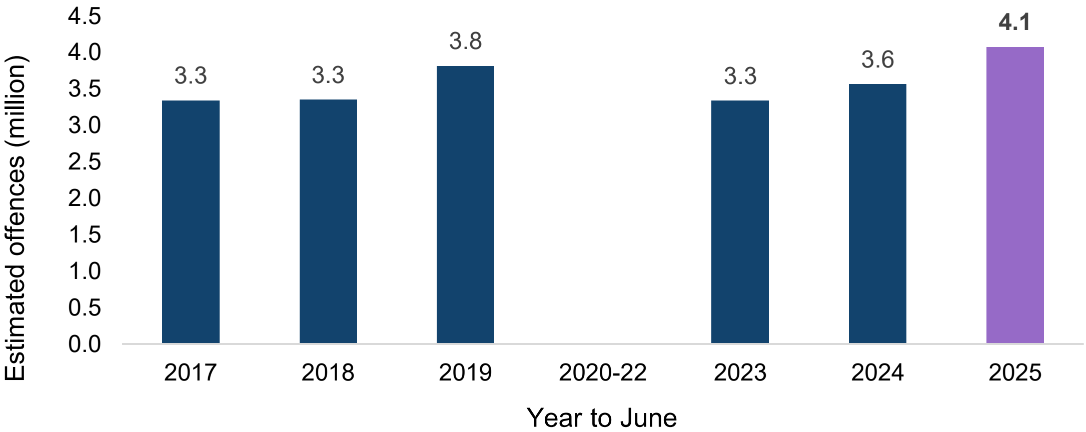
145. Today fraud is perpetrated with unprecedented speed and reach, and with minimal personal risk to the offender. Entrenched domestic obstacles, including a criminal justice system that is regrettably ill-equipped to respond with the necessary agility, only exacerbates matters. As a result, there is little to deter offenders.

146. The combination of system inertia and technological hyper-connectivity has rendered fraud an increasingly attractive proposition—a low-risk, high-reward activity, even for those who might never have considered breaking the law before. In this chapter, I briefly establish, through a quantitative lens, the current trajectory of the average fraud case as it progresses to, and through, the criminal justice system.

<u>Scale of Offending</u>

147. To understand why fraud has become so entrenched, we begin with its sheer scale, how frequently it occurs and how this trend has evolved over time. The Crime Survey for England and Wales (CSEW) estimates that fraud is, by some distance, the most frequently committed domestic crime, and it remains stubbornly so (see figure 1).[149] In the year ending June 2025, there were estimated to be 3.45 million victims. If, for the sake of illustration, each estimated offence represented one individual victim, there would be enough yearly fraud victims to fill all 20 Premier League football stadiums, five times over.[150]

Fig.2 – Fraud offending is substantial and increasing



[149] See 'Introduction' to this Review.

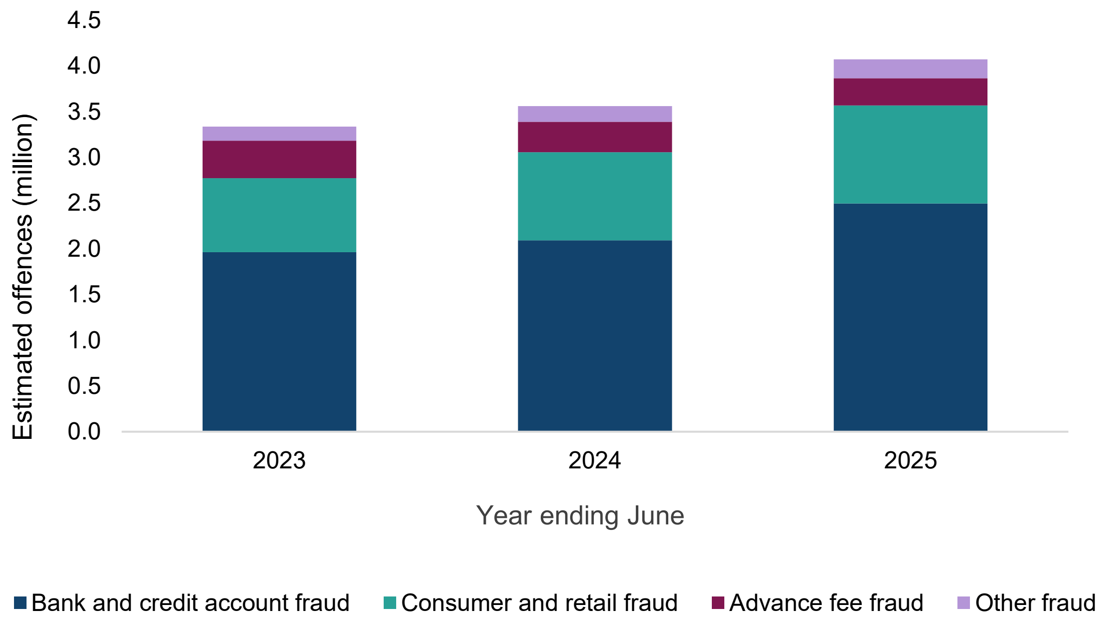
[150] Total capacity of all Premier League Football stadiums combined is approximately 800,000 seats.

148. This rise in fraud is not a blip. The data reveals a troubling pattern of substantial and steadily increasing criminal activity (see figure 2).[151] More concerning still, this Review heard evidence suggesting that, without strong action, fraud could constitute half of all crime in the United Kingdom (UK) by 2028. The stakes are exceptionally high.

Fraud Types

149. Yet scale alone does not tell the full story. The diversity of fraud types reveals why enforcement is complex and why victims are exposed to such varied risks. It would therefore be inaccurate to regard the estimated 4.1 million fraud offences as constituting a single, uniform type. While deception with intent to gain remains the core element, the methods by which fraud is committed vary widely (see figure 3).[152] Today, fraud is broadly categorised into two principal types: unauthorised and authorised.

Fig.3 – Fraud offending is not homogeneous



150. Unauthorised fraud occurs when a criminal gains access to a victim's bank account or payment card and makes transactions without their consent, typically using stolen credentials or through hacking.

151. Authorised fraud, by contrast, is more insidious. Here, the victim is deceived into making a payment themselves, believing it to be legitimate. Common examples include transferring money to a fraudster impersonating a bank, solicitor or family member.

---

151 Office for National Statistics, *Statistics on Crime in England and Wales*, (2025), Estimated fraud incidents, year ending June 2025. Note: direct comparison between 2016-2019/2023-2025 CSEW data and 2020-2022 TCSEW is not possible due to methodology changes caused by COVID.

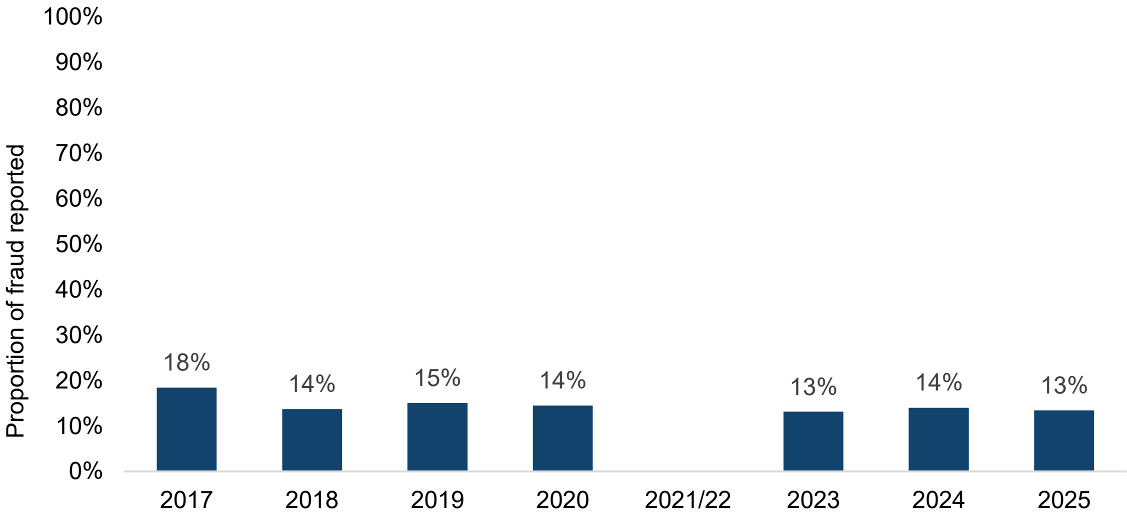
152 Office for National Statistics, *Statistics on Crime in England and Wales* (2025), (T)CSEW estimated fraud incidents, year ending June 2025.

Within these categories are numerous sub-types, including investment scams, romance fraud and invoice redirection. Many of these methods would be considered authorised push payment (APP) fraud, where victims 'authorise' a payment from their bank to a criminal posing as a trusted person or entity.

Under-Reporting

152. The first step once a fraud offence has been committed is for the authorities to become aware of the incident. The primary way this is achieved is by a victim making a formal report of criminal activity.[153] Yet only a limited proportion of offences are reported to Action Fraud, now Report Fraud, the national reporting service, or a local police force (see figure 4).[154] Without such reports, opportunities to pursue offenders and support victims are severely limited.

Fig.4 – Majority of fraud incidents are not reported



153. This gap between estimated offences and those recorded through official channels creates a serious intelligence deficit. It hampers both strategic planning and operational response. Data from the CSEW indicates that, in the year ending March 2025, only 13% of frauds committed in England and Wales were formally reported.

154. This gap is further complicated by the nature of the data that is reported. Of the approximately 300,000 reports submitted to Action Fraud, a proportion are duplicates, arising where both a victim and an institution, such as Cifas or UK Finance, report the same incident.

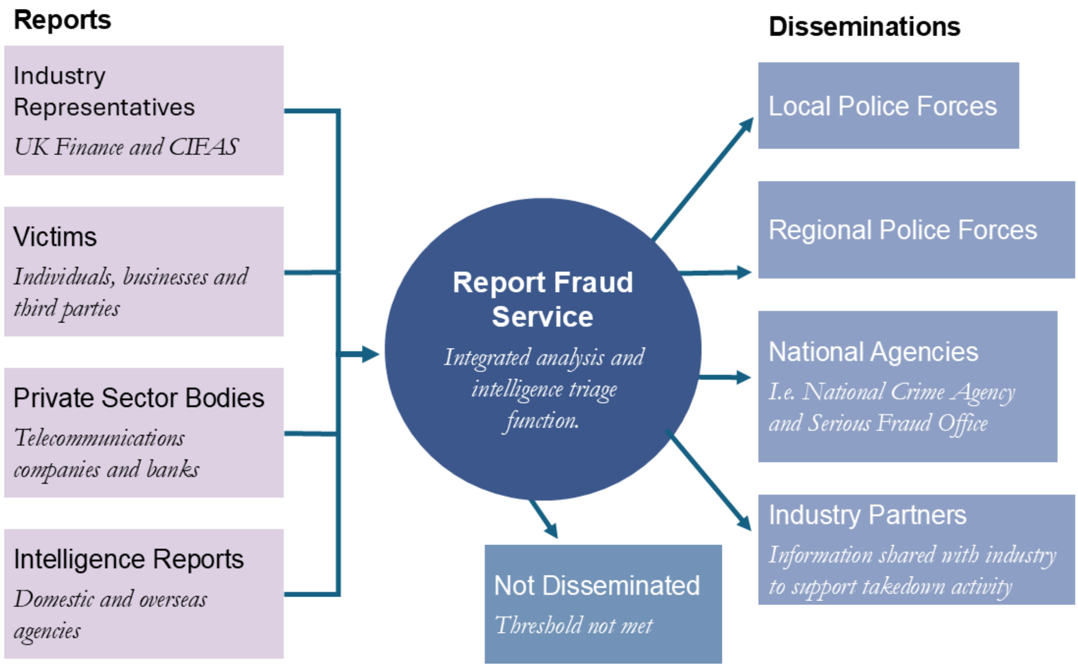
---

153 See chapter 'Detection and Disruption'.

154 Figure 3 – Ibid. CSEW – Proportion of fraud reported to Action Fraud or the Police, year ending March 2025. Estimated fraud incidents, year ending June 2025. Note: direct comparison between 2016-2019/2023-2025 CSEW data and 2020-2022 TCSEW is not possible due to methodology changes caused by COVID.

155. The Report Fraud analysis and intelligence function (formerly the National Fraud Intelligence Bureau (NFIB)) assess the viability of each report and, where appropriate, disseminates intelligence packages to the relevant investigative force (see figure 5). These packages may also be shared with industry partners to facilitate takedown and prevention actions, such as removing fraudulent websites or suspending bank accounts.[155] Only reports that meet the threshold (adequate detail, evidential basis, and actionable leads) are referred to police forces; those that do not, are not sent.

Fig.5 – Process of reports to and through the new Report Fraud service

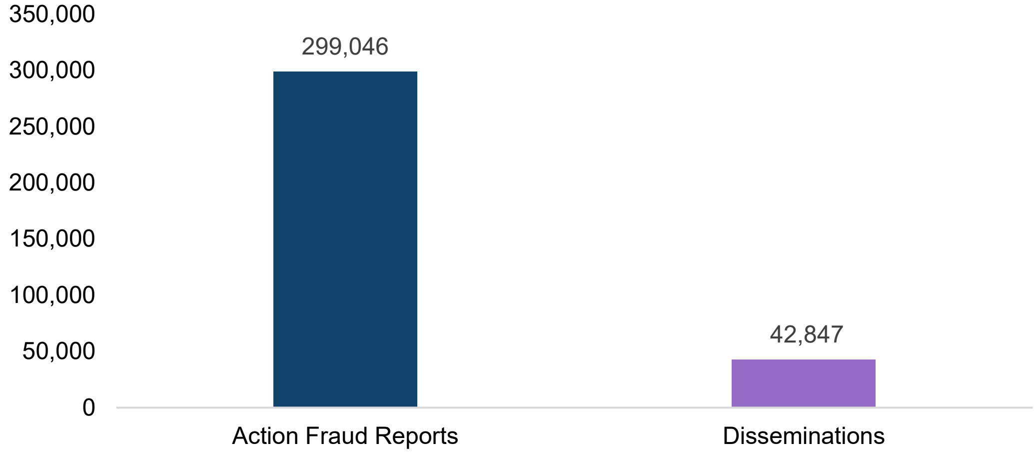


156. Of those cases that do satisfy the required criteria, only a minority proceed further. Of the thousands of fraud reports submitted, only 14% are ultimately disseminated to local police forces for consideration (see figure 6).[156] In the year to March 2025, one dissemination occurred for approximately every seven reports. This narrowing process demonstrates the practical constraints faced by enforcement agencies and highlights the challenge of translating reported incidents into investigative outcomes.

[155] City of London Police, *Written Evidence to the Serious Crime Bill [HL]* , (2015), SC 09. [Accessed 17 September 2025].

[156] Office for National Statistics, *Statistics on Crime in England and Wales* (2025). There is a time lag between the submission of Action Fraud reports and their dissemination to police forces. Consequently, the disseminations shown in the graph do not directly correspond to the same set of reports presented in the figure and are likely from previous years.

Fig.6 – Only a fraction of fraud reports is disseminated to police forces



157. Yet the funnel narrows further. Of the cases deemed viable and disseminated by the NFIB to local police forces, only a minor share is ultimately taken forward as criminal investigations. Of those disseminated, 80% resulted in no further action. The principal reasons cited were evidential difficulties (48%) and challenges in identifying suspects (29%). Only 13% of fraud dissemination outcomes result in a charge or summons, equating to just one in every 54 reports.[157]

158. During the Review's enquiries, it became clear that the Government does not currently hold reliable data on the number of live fraud investigations[158] underway across law enforcement. This is a critical gap in operational intelligence. Without it, it is extremely difficult to diagnose where the barriers lie between the dissemination of intelligence and the successful pursuit of investigations—and equally difficult for policymakers and enforcement agencies to assess whether current or future measures are having any material impact on the volume or quality of fraud investigations.

159. While some agencies have begun using platforms to record investigation numbers, this remains far from standard practice. I therefore suggest that the Government take swift steps to work with the full range of investigative bodies to explore a consistent and accurate process for recording fraud investigations.

160. The present reality is that, even where reports meet evidential and procedural thresholds, the likelihood of enforcement action remains limited. Investigative capacity is stretched, and without a baseline understanding of how many cases are in progress, it is difficult to assess the degree to which fraud case attrition at the investigative stage is a primary blocker.

157 Home Office, *Crime outcomes in England and Wales: 2024 to 2025*, year to March 2025, table 5.3.

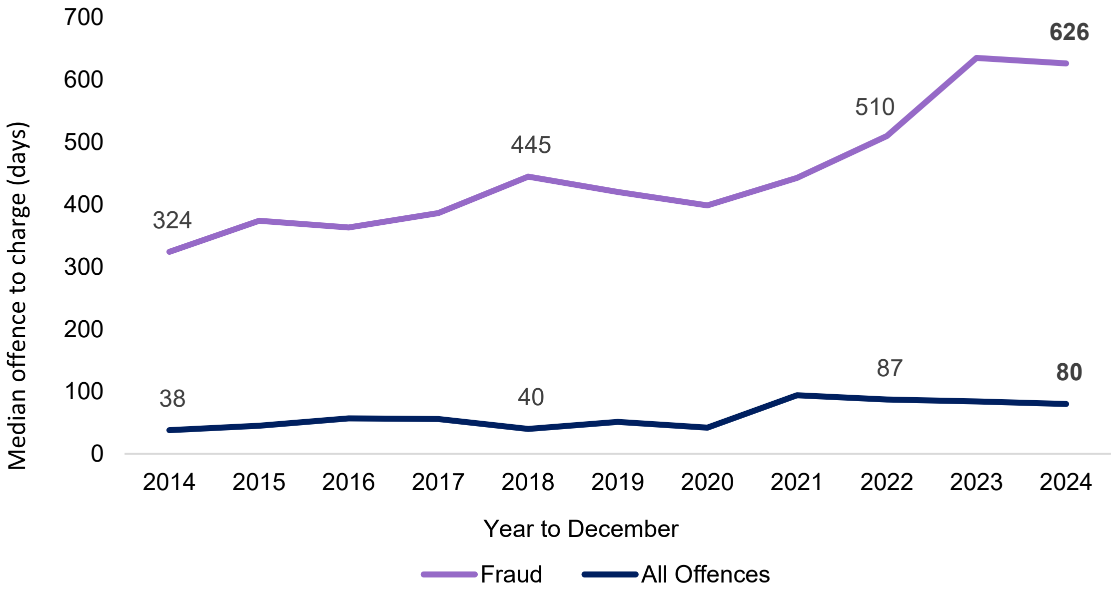
158 Offences committed against individuals and business, excluding fraud committed against the State.

Charging Decisions

161. Cases that progress to a charging decision face further obstacles. For victims whose cases reach the Crown Prosecution Service (CPS), the process is far from swift. In the year ending June 2025, the CPS made 9,450 decisions on fraud and forgery referrals.[159] While not an exact calculation, this figure supports the estimate that only around 20% of NFIB-disseminated cases ultimately mature into completed investigations that are subsequently submitted to the CPS for review.

162. The investigation and charge process is not expeditious. The average fraud victim waits over a year and a half, from the date of the offence to the charging decision date (see figure 7).[160] The disproportionate impact on fraud victims is shown most starkly when compared with the average criminal case (80-day average between offence and charge).

Fig.7 – Fraud victims wait an average of 1 year and 8 months for a charging decision



Court Progress

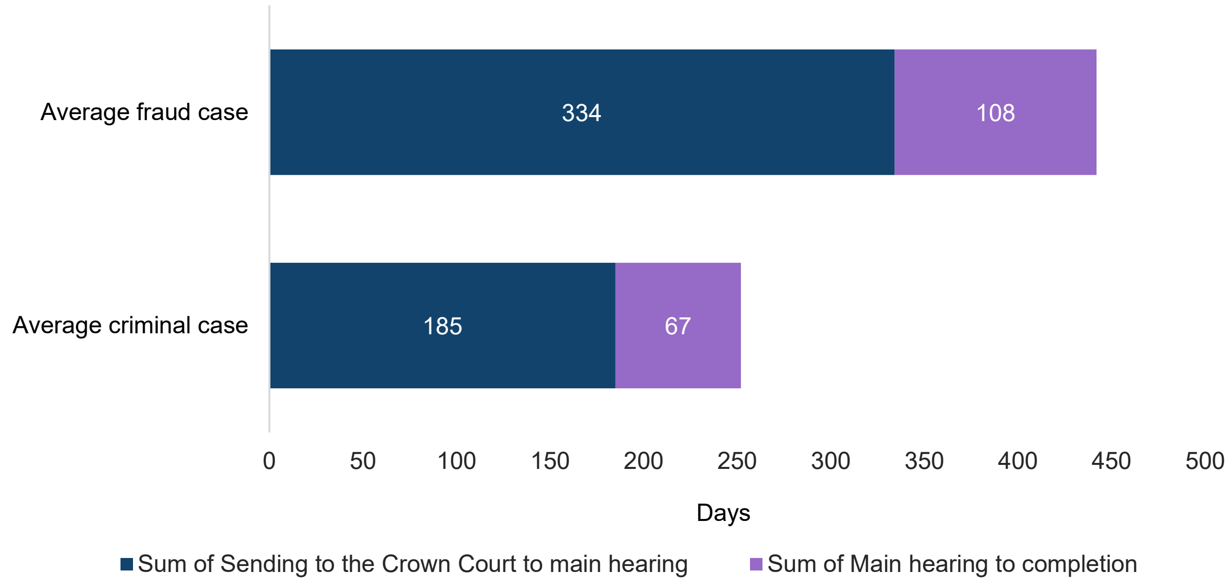
163. Substantial delays endure, if not increase, as fraud cases reach the criminal courts. On average, a fraud case takes almost twice as many days to reach first listing in the magistrates' courts (38.5 days), compared with the 'all crime' average (20 days).[161] The disparity only increases for those fraud cases deemed serious enough to be sent to the

[159] Crown Prosecution Service, *Pre-Charge Data Q1 2025-2026*, (2025), Tab 2.1, row 238. Of the total, 7,143 decisions were legal decisions (charge, no further action, out of court disposal etc.) and 2,304 were non-legal decisions.
[160] Ministry of Justice, 'End-to-end timeliness tool', in *Criminal court statistics quarterly January to March 2025*, (2025).
[161] Ibid.

Crown Court. It takes an average 442 days for a fraud case, once it has reached the Crown Court, to complete (see figure 8).[162]

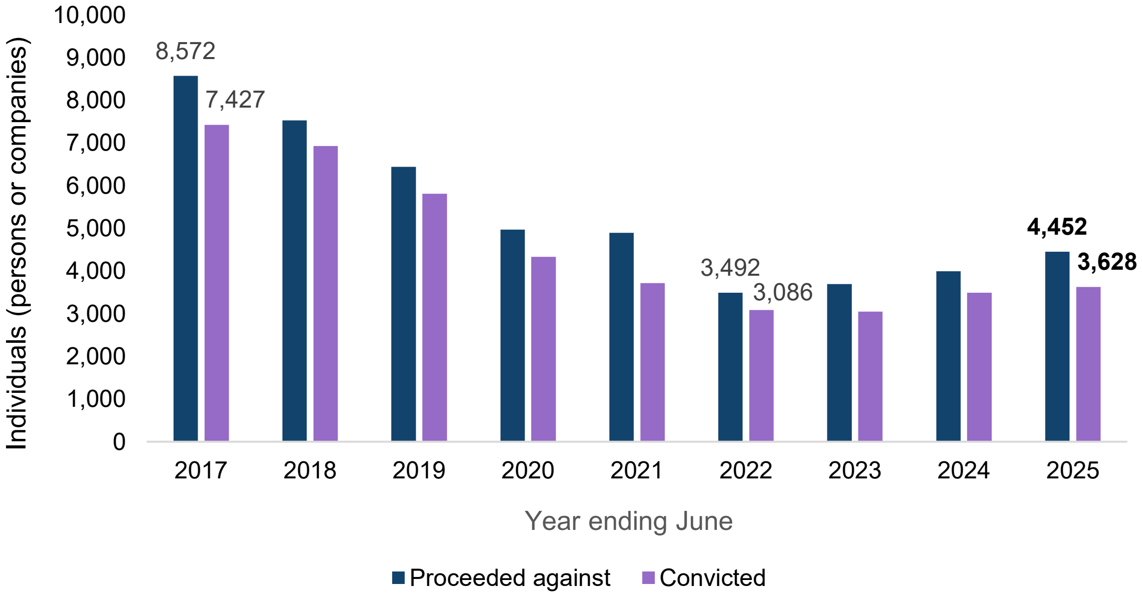
Fig.8 – More serious fraud cases crawl through Crown Court

Year to March 2025



164. The volume of fraud cases prosecuted by the CPS has also contracted markedly over time. Since 2017, there has been an estimated 60% reduction in the number of cases progressed to prosecution where fraud was the primary offence, although this decline appears to have stabilised in recent years (see figure 9).[163]

Fig.9 – Fraud prosecutions and convictions have decreased



162 Ibid, mean average.

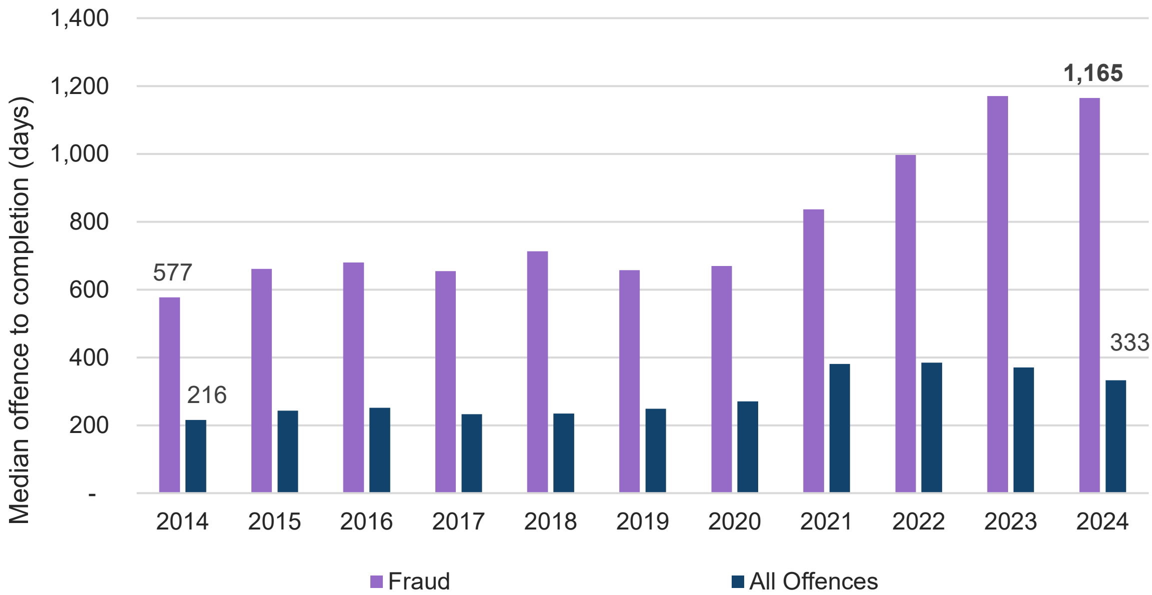
163 Ministry of Justice, *Outcomes by offence tool*, Criminal court statistics quarterly: January to March 2025 publication.

165. Conversely, the conviction rate for fraud remains robust: in the year ending March 2023, the CPS secured convictions in 83.9% of fraud prosecutions, marginally above the overall conviction rate of 83.1% for all crime.[164] This suggests that, while fewer cases are pursued, those that do proceed are generally well founded.

Conclusion

166. The data in this chapter speaks plainly. Fraud is no longer a peripheral offence; it is a dominant feature of modern criminality. The figures are stark: millions of estimated offences, yet only a fraction reported, and fewer still prosecuted. Of those that reach court, delay is the norm. For most victims, justice is distant, if it comes at all (see figure 10).[165]

Fig.10 – Fraud victims wait an average 1,165 days between offence to court completion



167. Convictions and court outcomes are not the sole measure of justice in fraud cases. Civil remedies, regulatory action and out-of-court disposals have a role, particularly given the pressures on the criminal justice system. Yet, if public confidence is to endure, the criminal courts must remain the central route of redress. That principle cannot be abandoned, even as more creative methods are explored.

168. The insights here show a system under strain: significant attrition at every stage, timeliness measured in years, and outcomes that fall far short of the scale of harm. These realities demand scrutiny and reform. It is those issues, and the options for change, that I examine in the chapters that follow. The present state of affairs is lamentable and cries out for reform.

---

[164] Ibid. NFIB-included offences: 51, 52, 53.4, 53.6, 53B.1, 53C, 53D, 53E, 53F.

[165] Ministry of Justice, '[End-to-end timeliness tool]', in *Criminal court statistics quarterly: January to March 2025,* (2025).

4. Enablers and Connected Criminality

169. Having set out the seismic scale of fraud and the faltering response of the criminal justice system, I now turn to the forces that are enabling its relentless proliferation. In this chapter, I locate fraud within a wider web of criminality. Fraud is rarely an isolated act.[166] It is often preceded by preparatory actions, such as data theft or cyber intrusion, and followed by the laundering and dispersal of criminal proceeds. It serves as both a gateway and a generator: a means by which individuals seeking a quick profit, and organised criminal gangs alike create revenue to sustain and expand their offending.[167]

170. I find that the same digital systems that enrich daily life, banking apps, cloud platforms, social media, video-calling, also furnish offenders with low-cost tools to find victims and deceive them at scale. Four central factors emerge as the principal drivers of this rise, each compounding the challenge faced by enforcement and policy makers alike:

    a. A low bar to entry.

    b. Greater opportunities to engage potential victims.

    c. Insufficient law enforcement engagement.

    d. The enthusiastic interest of organised crime.

<u>A Low Bar: Crime-as-a-Service</u>

171. Modern offending sits within a marketplace of suppliers, brokers and buyers. In this market, would-be offenders can acquire skills, scripts and services without deep technical knowledge. Social platforms, private forums and encrypted messengers provide recruitment, reputation and after-sales support.[168]

172. This ecosystem resembles a franchise model. A small cadre develops new exploits or techniques. A larger group 'packages' these tools hosting infrastructure, user dashboards, payment rails, and helpdesks. Finally, a mass of low-skilled consumers purchases or rents the 'product' to execute scams.[169] In effect, capability is modularised and commoditised.

---

[166] Harding, N., et al., 'The Liminality of Fraud: Reimagining Fraud Theory to Inform Financial Crime Prevention', *The British Journal of Criminology*, vol. 65, no. 3, 2025, pp. 618–638.
[167] United Nations Office on Drugs and Crime, *Global Report on Trafficking in Persons 2022*, (2022), page 102.
[168] Collier, B. and Hutchings, A., 'Cybercrime: A social ecology', in A. Liebling, S. Maruna & L. McAra (Eds.), *The Oxford Handbook of Criminology* (7th ed.), Oxford University Press, (2023).
[169] Ibid.

173. These activities are amplified by the increasing use of artificial intelligence (AI), which is playing an ever more prominent role in fraud facilitation. A survey by the Ada Lovelace Institute revealed that 58% of respondents had encountered AI-enabled financial fraud.[170]

174. Generative models can craft bespoke lures and deepfake voices and faces, and translate scripts for multiple demographics. Crime-as-a-service vendors provide a plethora of products for fraudsters from "pre-made malware to templates for phishing emails, payment processing systems and even helplines to enable bad actors to mount attacks with limited technical knowledge".[171] The advances in technology play a key role in lowering the threshold for fraud and in extending the reach of fraudsters.

175. Below are several current fraud-enabling technologies:

a. Caller and sender ID spoofing allows criminals to impersonate trusted institutions, banks, retailers, government bodies, by mimicking official phone numbers, branding and reply-paths. The result is a veneer of legitimacy that deceives even cautious victims.

b. Virtual Private Networks (VPNs) mask the true location of offenders, frustrate geolocation-based detection and allow overseas actors to present as operating within the United Kingdom (UK).

c. Voice over Internet Protocol (VoIP) enables high-volume calling at minimal cost. Offenders can rotate numbers rapidly and bypass carrier-level checks, making it harder to trace or block their activity.

d. Crypto-assets, such as Bitcoin, Ethereum and other digital tokens, offer fast, cross-border value transfer without traditional financial intermediaries. They provide pseudo-anonymity and agility, making them attractive for laundering the proceeds of fraud.

176. The bar to entry is now perilously low—not only because the requisite skills are minimal, but because many of these tools are easily accessible on the 'open' web.[172] There is no longer any need to delve into the dark web; the machinery of modern fraud is just a few clicks away to anyone with a smartphone, tablet or computer.

---

170 Ada Lovelace Institute, '7 in 10 says laws and regulations would increase their comfort with AI amid rising public concerns, national survey finds', press release, 25 March 2025.

171 Heinemeyer, M., 'Defending Against the New Normal in Cybercrime: AI', Darktrace, 7 March 2024, [Accessed 18 October 2025].

172 Open web – The publicly accessible portion of the internet that can be indexed by search engines and viewed without special permissions or encryption barriers.

Disrupting Marketplaces

177. Under section 6 of the Fraud Act 2006, possession of fraud-enabling products[173] (FEPs) is already a criminal offence. Yet the triable-either-way architecture dissuades investigators and prosecutors, with many cases not pursued, or consigned to delay, and the reality is stark, justice often never arrives.[174] Against this backdrop, the notion of prosecuting thousands of FEP purchasers identified in major operations is illusory.

178. Meanwhile, the threat landscape has shifted dramatically. Fraud forums and marketplaces operate at industrial scale. This Review heard evidence that, in 2024, every second a new advert for crime-as-a-service was placed online, with over 40 million adverts posted between 2023 and 2024. These figures underscore a simple truth: the machinery of modern fraud is not just hidden in the shadows of the dark web, it is marketed openly, with tutorials, user reviews and discount packages.[175]

179. Law enforcement has demonstrated its capacity to dismantle criminal infrastructure through operations such as Elaborate[176] and Stargrew. The latter alone exposed 2,000 active fraudsters harming 70,000 UK victims.[177] Yet these successes reveal a structural dilemma: when a single takedown yields thousands of identified purchasers, the resource burden of pursuing each through the criminal courts is prohibitive. In consequence, the vast majority escape sanction, and the criminal marketplace endures.

180. This is the moment to pivot, to raise the bar of entry to fraudulent offending. The objective must be twofold: first, to strike at the infrastructure by dismantling the marketplaces that sustain fraud; second, to reshape the decision-making process of those would-be offenders to think again before they act. If the act of purchasing a FEP carries a swift, certain consequence, even short of prosecution, the calculus of risk changes. Civil penalties offer that mechanism. They are not a dilution of criminal law but a complement to it: a means of imposing proportionate sanctions at scale.

181. The proposal is straightforward. The act of paying funds to acquire a fraud-enabling product, already unlawful, should attract a civil fine, issued administratively and enforced with the same rigour as other regulatory penalties. Such a regime could draw on provisions in the Public Authorities (Fraud, Error and Recovery) Act 2025[178] and the Digital Markets, Competition and Consumers Act 2024,[179] while reserving criminal prosecution for the

---

173 Fraud-enabling product – A software application, digital tool or service primarily designed or marketed to facilitate the commission of fraud, including but not limited to, to identity spoofing, phishing, credential harvesting, or impersonation of legitimate entities.
174 See chapters 'Contemporary Picture' and 'Courts'.
175 Vu, A.V., et al., 'Turning up the dial: The evolution of a cybercrime market through set-up, stable, and Covid-19 eras', in Proceedings of the Association for Computing Machinery Internet Measurement Conference 2020, pp. 552–556.
176 Met Police, 'Operation Elaborate', (updated April 2023), [Accessed 31 October 2025].
177 BBC One Morning Live, 'Operation Stargrew', (2024), [Accessed 31 October 2025].
178 Public Authorities (Fraud, Error and Recovery) Act 2025, s. 51.
179 Digital Markets, Competition and Consumers Act 2024, s.229.

gravest cases. This approach would enable law enforcement to act decisively during major operations, targeting hundreds or thousands of identified purchasers without overwhelming the courts, and signalling unequivocally that the purchase of FEPs is not a low-risk enterprise, but a sanctionable act.

182. It is right to acknowledge the practical challenges inherent in such a regime. While new or would-be offenders may be deterred, serious offenders are unlikely to be dissuaded. Identifying purchasers of FEPs will require investigative effort, and a proportion of individuals, those based internationally, will inevitably seek to evade payment. A proportion will contest penalties, necessitating a clear and accessible route of appeal. These considerations are real, but they are not insurmountable.

183. Civil enforcement mechanisms, supported by established debt recovery processes and County Court judgments, can deliver meaningful deterrence. Crucially, the availability of a civil penalty must not foreclose the option of criminal prosecution where the gravity of conduct warrants it. The civil route is not a substitute for justice; it is an additional instrument, enabling law enforcement to act swiftly and proportionately without surrendering the capacity to pursue criminal prosecution and custodial sentences in serious cases.

Recommendation 1

Grant law enforcement the power to issue civil fines to individuals purchasing fraud-enabling products online, drawing on provisions in the Public Authorities (Fraud, Error and Recovery) Act 2025 [Chapter 5]. Law enforcement should also retain discretion to pursue prosecution and custodial sentences in serious cases.

Exposure of Potential Victims

184. Compared with 50 years ago, our exposure to fraud has grown exponentially. In the past, a fraudster would need to knock on your door, intercept you in the street, work alongside you in an office, or capture your attention through a newspaper advertisement. Today, that same fraudster can reach you, and billions of others, instantly, through the immense and borderless reach of social media.

185. This exposure is compounded by the accessibility of personal data, which enables fraudsters to tailor their attacks with precision. Successful scams are rarely random. Offenders use personal information to craft convincing pretexts, refine timing and increase credibility. The breach of such data, whether through legitimate brokers or illicit markets, has become a key enabler of modern fraud.

186. **Legitimate data brokers –** Data brokerage firms collect, aggregate and trade in vast quantities of personal information. While such activity may be lawful and can serve

legitimate purposes, supporting sectors such as advertising, credit-risk assessment and service design, the concern lies in the governance of these operations.

187. Weak mechanisms for obtaining consent, opaque data retention policies, inadequate security protocols and the onward sharing of data without meaningful oversight all heighten the risk of bulk data being leaked or misused. Particularly in the context of fraud, location and behavioural data is acutely sensitive, as it enables precise timing and high-yield social engineering. Given that many data brokers operate across borders, there is a compelling case for international cooperation to strengthen security standards and minimise the risk of breaches.

188. **Illicit data brokers –** Alongside the legitimate market exists a shadow economy of illicit data brokers who employ a range of techniques to steal personal information and then trade or sell it, often on the dark web. This stolen data is typically listed and priced according to its freshness and geographic relevance. Such practices allow even low-skilled operators to select targets with pre-validated identifiers, significantly increasing the success rate of phishing attacks, business email compromise and investment scams.

189. Data stealing techniques include:

a. **Credential dumps** – This is a technique through which cybercriminals hack into a device's Random Access Memory and search for whatever credentials they can find, such as usernames and passwords. Once they have secured this credential, they will attempt to 'escalate their privilege' and infect other devices connected on the same network.

b. **Credential stuffing** – Akin to credential dumps, this is a less sophisticated method which seeks to use stolen credentials on multiple websites in search for a vulnerability.

c. **SIM swaps** – A cyber-attack which allows fraudsters to masquerade as mobile carriers, enabling them to send text messages to individuals, thereby inducing victims into transferring their phone number to a new SIM card controlled by the criminal. Once successful, the criminal disables the victim's SIM and takes full control of their number. This allows them to intercept calls and texts, including security codes for banking and other services, and potentially send fraudulent messages or access sensitive accounts.

d. **Mixed breach compilations** – An attack where the fraudsters use a combined list of leaked credentials from multiple previous data breaches to gain unauthorised access to accounts.

Case Study – National Public Data Breach

In August 2024, the Florida-based data-broker company, National Public Data, one of the largest background check companies operating in the US, admitted to suffering a serious data breach in late December 2023. The breach, conducted by the cyber-criminal gang USDoD, enabled the criminal infiltrators access to nearly 3 billion personal records, including of citizens from Canada, the UK and the United States.

The information secured through the hack includes personal identifiers, such as individuals' social security numbers, which could be used to commit a range of frauds. Sophisticated fraudsters may use this data to craft messages to deceive the victims into providing further personal information or into an authorised push payment scam.[180]

190. Today, it is easier than ever for personal information to be harvested, traded and exploited deliberately by malicious actors and inadvertently by corporations whose data practices often lack transparency. Whilst there is a regulatory framework established to safeguard personal information, supported by codes of practice across various industries, there remains a serious threat posed by corporations, who hold substantial personal data, falling short of their responsibilities. The nature of personal data is such that, once leaked onto the internet, it is supremely difficult to prevent its onward transmission.

191. In recognition of the risks posed by this emerging sector, the Department for Science, Innovation and Technology conducted a call for evidence on how data brokerage practices may pose risks to UK national interests.[181] As noted above, the impact of the new sector stretches beyond national security concerns and must be considered a significant enabler to modern fraud.

Insufficient Law Enforcement Engagement

192. The response of UK law enforcement to fraud is examined in greater detail in the chapter 'Investigation'. However, it is necessary at this stage to acknowledge a persistent and problematic bias: fraud, particularly in its online forms, has long been perceived as less harmful than physical crime. This assumption, though increasingly challenged, is deeply embedded in the culture of frontline policing.[182] It has contributed to a reactive posture in which fraud is investigated only after the fact, and often with minimal resource allocation.

---

180 As outlined in *Hofmann v. Jerico Pictures, Inc.,* No. 0:24-cv-61383 (S.D. Fla. filed Aug. 1, 2024), [Accessed 23 November 2025].
181 Department for Science, Innovation and Technology, *Call for evidence: Data brokers and national security*, (2025), [Accessed 4 December 2025].
182 HM Inspectorate of Constabulary and Fire & Rescue Services, *Fraud: Time to Choose – An inspection of the police response to fraud*, (2023).

193. The under-prioritisation of fraud within policing is compounded by several structural challenges. First, the skill sets required to investigate complex frauds, particularly those involving digital infrastructure, cross-border transactions and encrypted communications, are not widely held within local police forces. Second, the investigative burden is substantial.

194. Fraud investigations are inherently complex and resource intensive. They frequently require extensive digital forensic analysis, prolonged surveillance, and coordination across multiple jurisdictions, often involving international partners. The procedural demands are equally burdensome. Disclosure obligations, in particular, impose significant strain: officers must examine vast volumes of digital and documentary material, extract relevant evidence, and compile comprehensive case files. These must then be submitted for charging decisions, a process which itself may be protracted. The cumulative effect is a substantial drain on time, personnel, and operational capacity, factors which, in turn, diminish appetite within law enforcement to pursue fraud cases.

<u>The Enthusiastic Interest of Organised Crime.</u>

195. A fourth factor driving the proliferation of fraud is the sustained and strategic interest shown by serious and organised crime groups. While early instances of hacking were often exploratory in nature, the digitisation of daily life has transformed online-enabled fraud into a lucrative and scalable criminal enterprise.

196. Cybercrime and fraud have evolved from niche activities into vast illicit industries. In some cases, state actors engage directly in cyber operations, while certain jurisdictions benefit, either tacitly or overtly, from the financial flows generated by fraud. The profitability of fraud, coupled with low enforcement risk and minimal entry costs, has made it an attractive proposition for criminal organisations.

197. Experts consulted during this Review describe a growing cohort of well-educated individuals entering fraud as a profession. These actors are often trained through so-called 'scam academies' and operate with a level of sophistication that belies their lack of formal qualifications. The barriers to entry are low, the rewards high, and the likelihood of prosecution, particularly across borders, limited.

198. Fraud is not merely opportunistic; for organised crime groups, it is strategic. It provides a dependable financial lifeline, fuelling further criminal enterprise, including drug trafficking, human exploitation and illicit trade.[183] [184] Previous governments recognised

[183] United Nations Office on Drugs and Crime, *Organized Fraud, Issue Paper,* (2024).
[184] Levi, M., 'Organized fraud and organizing frauds: Unpacking research on networks and organization', *Criminology & Criminal Justice*, vol. 8, no. 4, 2008, pp. 389–419.

this threat, incorporating fraud into their Economic Crime Plans[185] [186] and Serious and Organised Crime Strategy.[187]

199. While the precise link between fraud and organised crime remains difficult to quantify, research by the Police Foundation in 2016 estimated that between 31% and 45% of fraud investigated by local police forces was linked to Organised Criminal Groups (OCGs).[188] Other estimates place this figure as high as 90%, depending on the type of fraud and the victim's location.[189]

200. It has also been asserted that fraud is used to finance terrorism on UK soil; for example, the Irish Republican Army was known to use tax fraud to support its operations.[190] In certain cases, it often difficult to group terrorism together with organised crime. This is for two reasons.

a. **Incentive** – Organised criminal activity, such as drug-trafficking, is primarily driven by financial interest; however, terrorism differs, as the primary motive is not profit but the desire to impose one's radical political vision on others.

b. **Lone attackers** – Acts of terrorism are often perpetrated by radicalised individuals acting without specific directions from others.

201. Regardless of the classification, what is evident is that fraud can be used by either organisations or individuals, as is the case for the 2017 Manchester bomber, to finance violent attacks on our streets.[191]

202. A crime once perceived to be confined to contractual disputes[192] has evolved into a global enterprise with a low threshold for entry, vast reach and minimal deterrence. The tools of modern life, social media and instant communications, have become the instruments of fraud, enabling offenders to cast their nets across millions of potential victims.

203. Law enforcement, constrained by finite resources and competing priorities, has struggled to match the velocity of modern fraud. Investigations are intricate, disclosure obligations onerous, and justice—where achieved—arrives late. In this vacuum, fraud has become a magnet for opportunists and organised crime alike, embedded within a wider criminal ecosystem that feeds, and is fed by, other illicit trades. Yet there is an opportunity to pivot: to target not merely the fraud after the fact, but the machinery that enables it, the tools, products and platforms that sustain this illicit economy. By striking at these enablers, law enforcement can begin to dismantle this web of criminality one thread at a time.

---

185 Home Office and HM Treasury, *Economic Crime Plan 1: 2019-22*, (2019).
186 Home Office and HM Treasury, *Economic Crime Plan 2: 2023-2026*, (2023).
187 Home Office, *No Place to Hide: Serious and Organised Crime Strategy 2023-2028*, (2023), CP 992.
188 The Police Foundation and Perpetuity Research, *Organised Fraud in Local Communities*, (2016).
189 May, T. and Bhardwa, B., *Organised Crime Groups Involved in Fraud*, Basingstoke: Palgrave Macmillan, (2018), page 61.
190 Woodford, I. and Smith, M.L.R., 'The Political Economy of the Provos: Inside the Finances of the Provisional IRA – A Revision, *Studies in Conflict and Terrorism*, vol. 41, no. 3, 2018, pp. 213–240.
191 Ryder, N. *Written Evidence Submitted to the UK Parliament* , (2023), FRA0010.
192 See chapter 'Short History of Fraud'.

5. Legislative Landscape

204. As discussed in the chapter 'History of Fraud', fraud offences on the statute book today are the product of successive legal and policy responses to evolving forms of deception and abuse. In this chapter, I focus on the two most significant provisions for prosecuting fraud committed against individuals and businesses: the Fraud Act 2006 and the common law offence of conspiracy to defraud.

205. While these are the most prominent, it is important to acknowledge the broader legislative landscape, which includes a range of other offences capable of capturing fraudulent conduct, including:

    a. False accounting (section 17 Theft Act 1968).

    b. False statements by company directors (section 19 Theft Act 1968).

    c. Fraudulent trading (section 993 Companies Act 2006).

    d. Adjacent offences around bribery (Bribery Act 2010).

206. Among the most recent additions to the statute book is the Economic Crime and Corporate Transparency Act 2023 and the Online Safety Act 2023, which both contain antifraud provisions relating to the responsibility of companies and senior persons within organisations.

<u>The Fraud Act 2006</u>

207. The Fraud Act 2006, which came into effect on 15 January 2007, marked a pivotal shift in the United Kingdom's (UK's) approach to tackling fraud. By consolidating disparate offences into a single, general offence of fraud, the Act enabled prosecutors to respond more effectively to increasingly sophisticated deception. Its structure has proven adaptable to a wide range of fraudulent conduct.

208. Section 1 of the Act sets out the structure of the broad offence, specifying three ways in which the offence can be committed: by false representation, failing to disclose, and fraud by abuse of position. Each formulation is detailed in a subsequent section of the Act.

Fraud Act 2006

Section 1

(1). A person is guilty of fraud if he is in breach of any of the sections listed in subsection (2) (which provide for different ways of committing the offence).

(2). The sections are—

(a) section 2 (fraud by false representation),

(b) section 3 (fraud by failing to disclose information), and

(c) section 4 (fraud by abuse of position).

209. For each formulation to commit the offence, set out below, the defendant's conduct must be dishonest and carried out with the intention of making a gain or causing a loss—or exposing another to the risk of loss. In a clear departure from earlier statutory offences, the Fraud Act 2006 does not require that a gain or loss actually occurs; it is sufficient that there was intent to bring about such an outcome.

210. Section 5 of the Act defines 'gain' and 'loss' as relating solely to money or other property, whether temporary or permanent. 'Property' is broadly defined to include both real and personal property, encompassing things in action and other intangible assets.

Fraud Act 2006

Section 2 – Fraud by false representation

(1) A person is in breach of this section if he—

(a) dishonestly makes a false representation, and

(b) intends, by making the representation—

(i)to make a gain for himself or another, or

(ii)to cause loss to another or to expose another to a risk of loss.

(2) A representation is false if—

(c) it is untrue or misleading, and

(d) the person making it knows that it is, or might be, untrue or misleading.

(3) "Representation" means any representation as to fact or law, including a representation as to the state of mind of—

(e) the person making the representation, or

(f) any other person.

(4) A representation may be express or implied.

Fraud Act 2006

Section 3 – Fraud by failing to disclose information

A person is in breach of this section if he—

(a) dishonestly fails to disclose to another person information which he is under a legal duty to disclose, and

(b) intends, by failing to disclose the information—

(i)to make a gain for himself or another, or

(ii)to cause loss to another or to expose another to a risk of loss.

Fraud Act 2006

Section 4 – Fraud by abuse of position

(1) A person is in breach of this section if he—

(a) occupies a position in which he is expected to safeguard, or not to act against, the financial interests of another person,

(b) dishonestly abuses that position, and

(c) intends, by means of the abuse of that position—

(i)to make a gain for himself or another, or

(ii)to cause loss to another or to expose another to a risk of loss.

(2) A person may be regarded as having abused his position even though his conduct consisted of an omission rather than an act.

Fraud Act 2006

Section 5 – "Gain" and "loss"

(1) The references to gain and loss in sections 2 to 4 are to be read in accordance with this section.

(2) "Gain" and "Loss"—

(a) extend only to gain or loss in money or other property;

(b) include any such gain or loss whether temporary or permanent;

and "property" means any property whether real or personal (including things in action and other intangible property).

(3) "Gain" includes a gain by keeping what one has, as well as a gain by getting what one does not have.

(4) "Loss" includes a loss by not getting what one might get, as well as a loss by parting with what one has.

211. Section 6 creates a wide criminal offence which applies where a person possesses any article with the intention that it be used in the course or in connection with fraud. Section 7 applies to those who create, adapt, supply or offer to supply articles for use in fraud, and clarifies that 'article' includes any program or data held in electronic form. The Act also created a new offence of fraudulent trading (section 9), which only applies to those businesses beyond the reach of the fraudulent trading offence in the Companies Act 2006 and obtaining services dishonestly (section 11).

Fraud Act 2006

Section 6 – Possession etc. of articles for use in fraud

(1) A person is guilty of an offence if he has in his possession or under his control any article for use in the course of or in connection with any fraud.

Fraud Act 2006

Section 7 – Making or supplying articles for use in frauds

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article—

(a) knowing that it is designed or adapted for use in the course of or in connection with fraud, or

(b) intending it to be used to commit, or assist in the commission of, fraud.

212. In addition to the Fraud Act's core offences (sections 2–4), two further significant fraud offences require explicit treatment in this Review's legal framework. First, the common law offence of cheating the public revenue, preserved when the general offence of 'cheat' was abolished in 1968, remains a potent instrument in serious tax and revenue cases. It does not require a positive act of deception; dishonestly failing to account or submit returns can suffice where the conduct prejudices HM Revenue and Customs' right to tax (e.g. *R v Mavji*;[193] *R v Hudson*[194]) and the mental element is intention (knowledge or wilful blindness) rather than recklessness (e.g. *R v Godir* [195]). Sentencing is uncapped at common law, with very substantial custodial terms imposed in grave cases.

213. Second, section 9 of the Fraud Act 2006 extends fraudulent trading to non-corporate businesses (sole traders, partnerships and other entities outside Companies Act s.993). The offence captures knowing participation in a business carried on "with intent to defraud creditors of any person or for any other fraudulent purpose" and carries a maximum of ten years' imprisonment. Its purpose is to close the gap where comparable conduct would previously have been beyond corporate fraudulent trading provisions.

214. Section 2 of the Criminal Justice Act 1993, as amended by the Fraud Act 2006, confers extraterritorial jurisdiction where any relevant constituent event occurs in England and Wales. This applies to various fraud and dishonesty offences, including offences contrary to sections 1, 6, 7, 9 and 11 of the Fraud Act 2006. Specifically, the courts in England and Wales will have jurisdiction to try a Fraud Act offence if, for example, part of the false representation, or any gain or loss, occurred in England and Wales. The maximum custodial sentence for an offence under section 6 is five years, and for sections 2, 3, 4 and 7 it is ten years.

215. Since its enactment, the Fraud Act 2006 has been subject to several evaluations, most notably the post legislative assessments in 2012[196] and 2022.[197] Both assessments concluded that the Act remains fit for purpose, broad enough to capture most forms of fraudulent offending and adaptable to evolving technologies.

216. The House of Lords Select Committee for the Fraud Act and Digital Fraud concluded: "the Fraud Act 2006 is a sound piece of legislation that is not in need of substantial reform. However, its efficacy is hindered by wider issues relating to its use in the prosecution of fraud cases and shortfalls in the prevention and detection of fraud, and enforcement of the legislation."[198]

---

193 *R v Mavji* [1987] 84 Cr App R 34; [1987] 2 All ER 758 (CA, 24 June 1986).

194 *R v Hudson* [1956] 2 QB 252 (Court of Criminal Appeal).

195 *R v Godir* [2018] EWCA Crim 2294 (CA, 11 October 2018).

196 Ministry of Justice, Post-Legislative Assessment of the Fraud Act 2006: Memorandum to the Justice Select Committee. (2012), Cm 8372.

197 Ministry of Justice, Post-Legislative Assessment of the Fraud Act 2006: Memorandum to the House of Lords Select Committee for the Fraud Act and Digital Fraud. (2022), Cm 680.

198 House of Lords, Fighting Fraud: Breaking the Chain: Fraud Act 2006 and Digital Fraud Committee, (2022), HL 87.

217. While the Fraud Act 2006 has been praised for its clarity, flexibility and effectiveness in prosecuting a wide range of offences, alongside these positive assessments the Fraud Act has also attracted criticism, particularly for being overly broad and potentially open to misuse. When it was first enacted, the most prominent concern was that it risked 'criminalising lying', particularly under section 2 (fraud by false representation).[199] Critics have also voiced concern over the Act leading to over-criminalisation by capturing activity deemed to be dishonest.

218. Although the Fraud Act 2006 provides a clear statutory framework, its effective application depends on precision in pleading. It is vital that prosecutors draft the particulars of any alleged false representation with the utmost clarity, leaving no room for ambiguity as to meaning. Failure to do so risks undermining the integrity of the charge, as emphasised in judicial scrutiny such as *R v Sharma*.[200]

219. While concerns have been raised in some quarters, they were not widely reflected during my Review. Stakeholders generally endorsed the continued use of the Act, reporting few practical difficulties with its application. On the contrary, many considered it a well-drafted statute that effectively addresses the types of offending currently encountered. So much so that the Fraud Act is being used in international fora to assist other jurisdictions as they consider what offences they might need to consider to tackle growing incidents of fraud in their own countries.[201]

220. In my assessment, the Fraud Act 2006 remains a robust and flexible piece of legislation. It continues to provide a clear framework for prosecution of a wide range of fraudulent conduct and, in my view, does not require amendment at this time. That said, a separate mischief has arisen that reduces the effectiveness of the offence, namely the time taken between the commission of a fraud offence and completion of trial at the Crown Court.[202] This substantial delay and the current state of the criminal justice system minimise the attractiveness and utility of the triable-either-way architecture.[203]

221. It is against this backdrop that I shall shortly examine two particularly salient and evolving forms of fraud which are taking place. First, I consider romance fraud and assess whether the Act is sufficiently equipped to address the unique and pernicious nature of these offences. Second, I explore a new fraud threat that has arisen since the last Fraud Act 2006 assessment, namely the growth in Artificial Intelligence- (AI-) enabled fraud and evaluate whether the current legislative framework is adequately future-proofed to respond to the challenges posed by emerging technologies.

---

199 Ormerod, D., 'The Fraud Act 2006 - Criminalising Lying?', *Criminal Law Review*, 1 Jan 2007, pp. 193–219.
200 *R v Sharma* [2025] EWCA Crim 1122. The Court of Appeal stressed the need for precise particulars of false representation under the Fraud Act 2006.
201 United Nations Office on Drugs and Crime, *Organized Fraud, Issue Paper,* (2024).
202 See chapter 'Contemporary Picture'.
203 See chapter 'Courts'.

Conspiracy To Defraud

222. Conspiracy to defraud is a common law offence in England and Wales, preserved by section 5(2) of the Criminal Law Act 1977. It remains a key prosecutorial tool in complex fraud cases, particularly where statutory offences under the Fraud Act 2006 may not adequately capture the scope or gravity of the criminal conduct. The maximum custodial sentence for conspiracy to defraud is ten years, aligning with the penalties available under the Fraud Act. The offence was defined in *Scott v Metropolitan Police Commissioner*.[204]

Conspiracy to Defraud

Common Law Offence
An agreement by two or more persons to dishonestly deprive a person of something to which they are entitled, or to injure some proprietary right of theirs.

223. The definition of the offence highlights its significant breadth, encompassing conduct that in isolation might not constitute an offence but which, by reason of two or more people agreeing to do it with the requisite intent, becomes an offence. To convict under this offence, there must also be intent to cause harm, which may include depriving someone of property or rights, injuring a proprietary interest, or cause someone to act against a public or legal duty. As with the Fraud Act, no actual loss or gain needs to occur.

224. The 2007 Attorney General guidelines regarding conspiracy to defraud state that a charge of statutory conspiracy should be brought in preference to a charge of conspiracy to defraud unless there are good reasons for doing otherwise. A charge of conspiracy to defraud may be appropriate where no charge of statutory conspiracy, or a substantive offence, could properly reflect the gravity of the offence, and/or where such charges might require a large number of separate counts or severed trials.

225. While law enforcement agencies find the offence useful in certain circumstances, the Law Commission fraud report[205] recommended abolishing it, arguing that the offence is uncertain and overly broad, with the potential to capture behaviour that should not be criminal. The Government chose not to proceed, citing strong opposition to that assessment in consultation responses. A further assessment in 2012 similarly concluded that the offence remained necessary and "essential", particularly in complex fraud cases involving multiple defendants and overlapping offences.[206] The 2022 assessment for the

[204] *Scott v Metropolitan Police Commissioner* [1975] AC 819.
[205] Law Commission, *Report on Fraud*, (2002), Report No. 276.
[206] Ministry of Justice, *Post legislative assessment of the Fraud Act 2006 - Memorandum to the Justice Select Committee*, (2012).

House of Lords Select Committee reaffirmed this position, noting that conspiracy to defraud continues to play a vital role in prosecuting fraudulent conduct.[207]

226. In the last year alone, there have been strong reminders of how this common law offence can be utilised, and misapplied. In *R v Hayes and Palombo* (2015), two traders were prosecuted for manipulating LIBOR and EURIBOR benchmark interest rates. Both had been convicted of conspiracy to defraud for dishonestly agreeing to submit rate estimates that favoured their trading positions. However, in 2025 the Supreme Court found that the trial judges had misdirected juries by treating the dishonesty of rate submissions as a matter of law, rather than fact.[208] The judges had wrongly instructed that any submission influenced by trading motives was inherently dishonest, removing the defendants' core defence. The Court clarified that rate submissions involved subjective judgment and that the honesty of such submissions should have been assessed by the jury. While the evidence could have supported convictions, the misdirection rendered the trials unfair.

227. Conversely, the recent case of *R v Skeene & Anor*[209] demonstrated the continued utility of the common law offence. The defendants, directors of Global Forestry Investments, were convicted of orchestrating a series of fraudulent investment schemes involving Brazilian teak plantations. From 2010 to 2015, they misled over 2,000 investors and raised £36.8 million by falsely claiming the schemes were ethical and profitable, when over £13 million was diverted into personal accounts.

228. The schemes were prolonged through the use of false documents, nominee directors, and deliberate deception of liquidators during the winding-up of their company. Prosecutors relied on conspiracy to defraud to capture the full scope of the dishonest agreement and coordinated conduct, which could not have been adequately reflected through individual charges under the Fraud Act 2006. On appeal, the Court of Appeal upheld the convictions, confirming that the indictment was sufficiently particularised and that the offence properly addressed the dishonest agreement to prejudice the proprietary rights of others.

229. Stakeholders consulted during the Review affirmed the value of conspiracy to defraud as a prosecutorial tool. While some practitioners noted they rarely relied on it, others, particularly those dealing with complex, multi-defendant or long-running fraud cases, emphasised its practical utility.

230. Prosecutors and investigators described the offence as essential in capturing dishonest agreements and coordinated conduct that falls outside the scope of statutory offences under the Fraud Act 2006. Across interviews, there was broad support for retaining the

---

[207] Ministry of Justice, *Post-legislative Assessment of the Fraud Act 2006 - Memorandum to the House of Lords Select Committee on the Fraud Act and Digital Fraud*, (2022), CP 680.
[208] R v Hayes and Palombo [2025] UKSC 29.
[209] *R v Skeene & Anor* [2025] EWCA Crim 17.

offence; however a minority of practitioners advocated for the Law Commission's position of abolishing the offence in light of *R v Hayes*.

231. Despite occasional debate about its necessity, I conclude that the offence should be retained, but its use should be carefully monitored to ensure it is applied proportionately and only where statutory alternatives are insufficient.

False Accounting and False Statements

232. While broader offences such as conspiracy to defraud can serve as a catch-all for complex fraudulent conduct, prosecutors often rely on statutory provisions to target specific criminal behaviour. One example is false accounting, under section 17 of the Theft Act 1968.

233. This offence is committed when a person, with intent to gain or cause loss, dishonestly destroys, defaces, conceals or falsifies any account, record or document required for accounting purposes, or uses such a document knowing it is misleading, false or deceptive in a material particular. False accounting is commonly prosecuted in cases involving internal financial manipulation or corporate fraud and carries a maximum sentence of seven years' imprisonment on conviction.

234. Closely related is the offence of false statements made by company directors, set out in section 19 of the Theft Act 1968. This provision criminalises the conduct of company officers who knowingly or recklessly publish, or concur in publishing, written statements or accounts that are misleading, false or deceptive in a material particular, with intent to deceive members or creditors about the company's affairs. It is designed to uphold transparency and integrity in corporate reporting and governance. Like false accounting, this offence carries a maximum penalty of seven years' imprisonment.

Theft Act 1968

Section 17 – False accounting.

(1) Where a person dishonestly, with a view to gain for himself or another or with intent to cause loss to another,—

(a) destroys, defaces, conceals or falsifies any account or any record or document made or required for any accounting purpose; or

(b) in furnishing information for any purpose produces or makes use of any account, or any such record or document as aforesaid, which to his knowledge is or may be misleading, false or deceptive in a material particular.

Section 19 – False statements by company directors, etc.

(1) Where an officer of a body corporate or unincorporated association (or person purporting to act as such), with intent to deceive members or creditors of the body corporate or association about its affairs, publishes or concurs in publishing a written statement or account which to his knowledge is or may be misleading, false or deceptive in a material particular, he shall on conviction on indictment be liable to imprisonment for a term not exceeding seven years.

Fraudulent Trading – 2006

235. These offences sit alongside other corporate fraud provisions designed to address dishonest business practices. One such offence is fraudulent trading, set out in section 993 of the Companies Act 2006. This offence applies where a person is knowingly party to the carrying on of a company's business with intent to defraud creditors or for any fraudulent purpose. It can be committed not only by directors but also by employees or third parties involved in the fraudulent conduct. Fraudulent trading is frequently prosecuted in the context of insolvency and commercial deception and carries a maximum penalty of ten years' imprisonment, a fine, or both.

Companies Act 2006

Section 993 – Offence of fraudulent trading

(1) If any business of a company is carried on with intent to defraud creditors of the company or creditors of any other person, or for any fraudulent purpose, every person who is knowingly a party to the carrying on of the business in that manner commits an offence.

(2) This applies whether or not the company has been, or is in the course of being, wound up.

Computer Misuse Act 1990

236. In contrast to offences under the Fraud Act 2006, which focus on dishonest conduct resulting in gain or loss, the Computer Misuse Act 1990 (CMA) targets the enabling actions that facilitate such criminality. The CMA was introduced following a Law Commission report on the misuse of computers which observed that current UK criminal offences had failed to keep pace with technological developments. It has since been amended, with new offences inserted, by the Police and Justice Act 2006 and Serious Crime Act 2015. The current computer misuses offences contained in the Act are:

a. **Section 1** – Criminalises unauthorised access to computer material—commonly known as hacking. It carries a maximum sentence of two years.

b. **Section 2** – Covers unauthorised access with intent to commit further offences. Essentially an aggravated form of Section 1. It carries a maximum sentence of five years.

c. **Section 3** – Targets unauthorised acts intended or reckless as to impairing computer operations. It carries a maximum sentence of ten years. The court confirmed in *DPP v Lennon* (2006)210 that section 3 is the appropriate charge in cases involving distributed denial of service (DDoS) attacks, a type of cyber-attack which renders a machine or network unavailable by flooding it with incoming traffic from multiple sources.

d. **Section 3ZA** – Introduced by the Serious Crime Act 2015, this offence addresses unauthorised acts causing or risking serious damage (e.g. to national infrastructure). It carries a maximum sentence of 14 years.

e. **Section 3A** – Criminalises the making, supplying, or obtaining of tools used to commit offences under Sections 1, 3, or 3ZA—such as malware. It carries a maximum sentence of two years.

237. The Review heard concerns from stakeholders regarding the overlap and ambiguity between the CMA and the Fraud Act, particularly in relation to impersonation, digital identity theft and data misuse. I also heard international engagement is complicated by inconsistent treatment of fraud as either cybercrime or economic crime. While both Acts may apply to similar conduct, their intentions differ.

238. The Fraud Act 2006 criminalises dishonest intent to secure gain or cause loss, whereas the CMA was enacted to safeguard computer systems from unauthorised access, including hacking, malware and other forms of criminal interference. Accordingly, this Review does not treat the CMA as a principal legislative instrument for addressing fraud. While reform of the CMA has been considered elsewhere, it falls outside the scope of this Review.

Bribery Act 2010

239. A further fraud-adjacent piece of legislation is the Bribery Act 2010, which modernised UK anticorruption law and introduced four principal offences: offering or giving a bribe (section 1), receiving a bribe (section 2), bribing a foreign public official (section 6), and failure of a commercial organisation to prevent bribery (section 7). The Act applies to individuals and companies and has extraterritorial reach, allowing prosecution of bribery committed abroad by UK-linked entities. Conviction can result in up to ten years' imprisonment, unlimited fines, and debarment from public contracts. As with the CMA, the performance of the Bribery Act is not considered by this Review.

[210] *DPP v Lennon* [2006] 170 JP 532.

6. Corporate Responsibility

240. This chapter continues the examination of the evolving legal framework designed to impose responsibility on organisations whose infrastructure facilitates fraud. It considers recent legislative developments, evaluates their scope and limitations, and explores whether further reform is warranted to close accountability gaps.

241. The offences discussed thus far focus primarily on individual conduct. However, there is growing recognition that fraud may be committed or facilitated by corporate entities. In recent years, concerns have intensified regarding the limited mechanisms available to hold companies criminally accountable for their role in enabling fraud.

242. In response, two key legislative developments have emerged. First, the Economic Crime and Corporate Transparency Act 2023 introduced a new corporate offence of 'failure-to-prevent' fraud, marking a significant expansion of criminal liability for organisations. Second, the Online Safety Act 2023 established a regulatory framework aimed at reducing online harm, including fraud, by imposing duties of care on digital platforms. While both measures seek to enhance corporate responsibility, they operate through distinct legal mechanisms—one criminal, the other regulatory.

<u>The Online Safety Act 2023</u>

The Online Safety Act 2023 represents a significant development in the regulation of online platforms. It imposes statutory duties of care on providers of user-to-user services (such as social media platforms) and search services accessible to United Kingdom (UK) users. These duties require platforms to take proactive steps to prevent users from encountering illegal content, including fraudulent material and content harmful to children.

243. This marks a departure from the previous legal framework, which was largely derived from the European Union's e-Commerce Directive and operated on a reactive 'notice and takedown' basis.[211] The Act introduces a new regulatory architecture, overseen by Ofcom, which is empowered to enforce compliance through civil penalties and binding codes of practice.

244. The legislation addresses a wide range of online harms, including specific provisions targeting fraudulent advertisement. Under the Act, platforms are required to conduct assessments for illegal content and implement safety-by-design features to mitigate fraud

[211] European Union, 'Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)', (2000), OJ L 178, 17.7.2000, pp. 1–16.

risks. Categorisation thresholds, laid alongside the Illegal Harm Codes in December 2024, set out the criteria for services to be designated as either Category 1, 2A or 2B.

Category 1

Category 1 platforms have the largest reach and influence across the UK population. The designation for Category 1 is:

(a) Platforms that use a content recommender system and have more than 34 million UK users (50% population) on the user-to-user part of the service; or

(b) Platforms that allow users to forward or reshare user-generated content and use a content recommender system and have more than 7 million UK users (10% population) on the user-to-user part of the service.

Category 2A and 2B

Category 2A applies to search services or a combined service. Additional requirements for these services, such as transparency and prevention of fraudulent advertising, will apply. The criterion for designation is if a platform:

(a) Has more than 7 million UK users (10% population); and

(b) Is not a vertical search engine (only enables a user to search selected websites or databases in relation to a specific topic, theme or genre of search content, such as a price comparison website).

Category 2B covers smaller categorised services. These services will only be required to conduct transparency reporting and have policies in place regarding the disclosure of information about use of the service by a deceased child user. A Category 2B service is one which:

(a) Allows direct messaging and has more than 3 million UK users (5% population).

245. Category 1 and Category 2A thresholds are set by the Secretary of State in secondary legislation, and services are designated by Ofcom (and subject to Ofcom codes of practice/guidance)—a structure deliberately chosen to pre-empt procedural challenges about threshold-setting and method compliance.[212]

[212] Department for Science, Innovation and Technology, *Explanatory Memorandum to The Online Safety Act 2023 (Category 1, Category 2a And Category 2b Threshold Conditions) Regulations 2025*, (2025), No. 226.

246. Sections 38 and 39 of the Act place particular obligations on the largest platforms (Category 1 and Category 2A),[213] requiring them to ensure that systems and processes are in place to prevent users from encountering fraudulent advertisements, minimise the duration such content remains online, and take prompt action to remove it once identified.

Online Safety Act 2023

Section 38 – Duties about fraudulent advertising: Category 1 services

(1) A provider of a Category 1 service must operate the service using proportionate systems and processes designed to—

(a) prevent individuals from encountering content consisting of fraudulent advertisements by means of the service;

(b) minimise the length of time for which any such content is present;

(c) where the provider is alerted by a person to the presence of such content, or becomes aware of it in any other way, swiftly take down such content.

Section 39 – Duties about fraudulent advertising: Category 2A services

(1) A provider of a Category 2A service must operate the service using proportionate systems and processes designed to—

(a) prevent individuals from encountering content consisting of fraudulent advertisements in or via search results of the service;

(b) if any such content may be encountered in or via search results of the service, minimise the length of time that that is the case;

(c) where the provider is alerted by a person to the fact that such content may be so encountered, or becomes aware of that fact in any other way, swiftly ensure that individuals are no longer able to encounter such content in or via search results of the service.

247. Ofcom is the designated regulator responsible for enforcing these duties and issuing Codes of Practice that outline recommended compliance measures. These include steps to prevent, detect and remove illegal content, as well as specific guidance on fraudulent advertising. If Ofcom determines that a platform is not doing enough, it has the authority to investigate and impose significant regulatory penalties. These can include fines of up to £18 million or 10% of global annual turnover, whichever is higher.[214] Ofcom also has

[213] Category definitions are set out in s. 95 of the Online Safety Act 2023.
[214] Online Safety Act 2023, schedule 13.

the power to apply business disruption measures, which in extreme cases could result in platforms being blocked in the UK.[215]

248. While the Act does not impose general criminal liability on directors, it does provide for personal criminal liability in specific circumstances. Under Part 7 and Part 10, senior managers may be prosecuted for offences such as failing to comply with an information or audit notice, or obstructing Ofcom's enforcement functions. These offences are narrowly defined and do not extend to failures in fraud prevention per se. Penalties may include imprisonment for up to two years.

249. The Online Safety Act represents a significant evolution in the regulation of online platforms, shifting from a reactive model, previously governed by the e-Commerce Directive, to a proactive regime of statutory duties of care. However, its scope remains regulatory rather than criminal, and its primary focus is on content moderation, risk assessments, and child safety.

250. It does not impose a direct duty on platforms to prevent fraud at the organisational level. In contrast, the failure-to-prevent fraud offence under the Economic Crime and Corporate Transparency Act 2023 introduces a corporate criminal liability model, requiring businesses to implement reasonable fraud prevention procedures. The absence of a comparable duty within the Online Safety Act may limit its effectiveness in addressing fraud unless supplemented by robust enforcement and cross-regulatory coordination.

Failure-to-Prevent Offence

251. Current failure-to-prevent offences comprise section 7 of the Bribery Act 2010, which covers failure to prevent bribery by an associated person, and sections 45 and 46 of the Criminal Finances Act 2017, which addressed failure to prevent the facilitation of UK or foreign tax evasion. From 1 September 2025, section 199 of the Economic Crime and Corporate Transparency Act 2023 introduced a new either-way, strict liability offence of corporate failure-to-prevent fraud.

252. Under this provision, large organisations can be held criminally liable if a person associated with them commits a fraud offence for their benefit, and the organisation lacks reasonable fraud prevention procedures. This offence mirrors the approach taken in the Bribery Act 2010, aiming to incentivise proactive fraud prevention within corporate structures.

[215] Online Safety Act 2023, Part 7, Chapter 6, Section 144: Business Disruption Measures.

Economic Crime and Corporate Transparency Act 2023

Section 199 – Failure to Prevent Fraud

(1) A relevant body which is a large organisation (see sections 201 and 202) is guilty of an offence if, in a financial year of the body ("the year of the fraud offence"), a person who is associated with the body ("the associate") commits a fraud offence intending to benefit (whether directly or indirectly)—

(a) the relevant body, or

(b) any person to whom, or to whose subsidiary undertaking, the associate provides services on behalf of the relevant body.

(2) A relevant body is also guilty of an offence under subsection (1) if—

(a) an employee of the relevant body commits a fraud offence intending to benefit (whether directly or indirectly) the relevant body,

(b) the fraud offence is committed in a financial year of a parent undertaking of which the relevant body is a subsidiary undertaking ("the year of the fraud offence"), and

(c) the parent undertaking is a relevant body which is a large organisation.

(3) But the relevant body is not guilty of an offence under subsection (1)(b) if the body itself was, or was intended to be, a victim of the fraud offence.

(4) It is a defence for the relevant body to prove that, at the time the fraud offence was committed—

(a) the body had in place such prevention procedures as it was reasonable in all the circumstances to expect the body to have in place, or

(b) it was not reasonable in all the circumstances to expect the body to have any prevention procedures in place.

253. Sections 199(1), Sections 201 and 202 apply to "relevant bodies" (corporate entities or partnerships) that qualify as large organisations, meaning they meet at least two of the following:

a. More than 250 employees.

b. More than £36 million turnover.

c. More than £18 million in total assets.

254. The application extends to companies if a subsidiary commits fraud for the parent's benefit (Section 199(2)). Under Section 199(4), the organisation can defend itself by proving that it had reasonable fraud prevention procedures in place, or it was not reasonable to expect such procedures in the circumstances. Section 199(5) sets out the prevention procedures, designed to prevent associated persons from committing fraud offences. The government has published guidance which explains what prevention procedures a reasonable corporate entity might have had in place, for each of the failure-to-prevent offences, and sets out six principles that organisations are expected to follow.[216]

255. One of the major barriers to prosecuting corporate fraud was the identification doctrine, which required proving that a company's 'directing mind and will' had the necessary criminal intent. In a 2022 comprehensive review on corporate liability, the Law Commission examined how domestic law holds companies to account for criminal conduct, including whether the identification doctrine is fit for purpose.[217] The review also considered the doctrine of *respondeat superior*, used in the United States to impose corporate liability for the actions of any employee acting within the scope of their employment.

256. While this represents a significantly broader basis for liability than the UK's current approach, the Law Commission opted instead to expand the identification doctrine through the introduction of the new 'failure-to-prevent' fraud offence. As this offence only came into effect on 1 September 2025 and its practical implications are yet to be tested, I have not assessed the merits of adopting a *respondeat-superior*-style regime at this stage. A more meaningful evaluation should be undertaken once the new offence has been implemented and its effectiveness reviewed.

257. Separately, Section 196 of the Economic Crime and Corporate Transparency Act (ECCTA) 2023 reforms the identification doctrine by introducing a new basis for attributing criminal liability to organisations. Prosecutors no longer need to prove that the individual was the 'directing mind and will' of the company. It is sufficient to show that a senior manager, defined as someone who plays a significant role in decision-making or management, acted within the scope of their authority. This reform is a deliberate shift toward a more realistic and enforceable model of corporate accountability.

---

216 Home Office, *Economic Crime and Corporate Transparency Act 2023: Guidance to organisations on the offence of failure to prevent fraud*, (2024).
217 Law Commission, *Corporate Criminal Liability: an options paper* , (2022).

Discussion

258. Having set out the new statutory architecture, it is necessary to consider its practical implications and whether the current framework delivers a coherent and proportionate response to the scale of online-enabled fraud.

259. The UK's legislative trajectory increasingly embraces corporate liability as a tool to combat economic crime. The Bribery Act 2010, the Criminal Finances Act 2017, and now the ECCTA reflect a growing consensus that businesses must take proactive steps to prevent criminal conduct. In this context, there is a compelling case for extending corporate liability to online platforms, particularly social media and search services, which play a demonstrable role in facilitating fraud.

260. In its 2022 report, the House of Commons Justice Committee explicitly recommended legislation requiring companies, including social media platforms, to prevent fraud on their systems.[218] The Committee noted that fraud is increasingly enabled through third-party infrastructure such as telecommunications, email and social media, and that prevention must be prioritised given the limited prospects for prosecuting foreign-based perpetrators. It concluded that a failure to-prevent-fraud offence would help focus private sector effort on "designing fraud out of companies' systems" and improving corporate culture.

261. Despite its significance, the ECCTA's scope is limited. Only an estimated 0.2% of UK businesses meet the statutory thresholds for large organisations.[219] Most UK companies are small and medium-sized enterprises (SMEs) and therefore fall outside the offence's reach. Moreover, many qualifying firms are already subject to Financial Conduct Authority's regulation and compliance frameworks,[220] potentially reducing the marginal impact of the new offence.

262. The offence applies to large organisations and only where fraud is committed by an associated person, such as an employee or agent, for the benefit of the organisation. It does not cover fraud committed by users of platforms, even where platforms profit from the traffic or advertising revenue generated by fraudulent content. This creates a substantial accountability gap. A broader failure-to-prevent fraud offence would help close this gap, incentivising platforms to implement robust fraud prevention systems and aligning responsibility across sectors.

263. Platforms increasingly host and monetise scam adverts, fake listings and other fraudulent content. While companies argue that identifying fraud is complex, particularly where it materialises off-platform or involves ambiguous content, this does not apply to the

[218] House of Commons Justice Committee, *Fraud and the Justice System*, (2022) HC 12, para 145.
[219] Gentle, S., 'Failure to prevent' rules unlikely to greatly impact fraud levels, *FT Adviser*, 1 September 2025.
[220] Financial Conduct Authority, *Handbook of Rules and Guidance*, (2025).

substantial volume of clearly fraudulent material that is openly hosted. In such cases, platforms are not passive intermediaries but active facilitators. The existence of grey-area content should not obscure the need for decisive action against obvious fraud.

264. By way of example, a recent Reuters investigation suggests that one of the world's largest technology platforms internally projected it could earn approximately 10% of its annual revenue, around US $16 billion, from advertising linked to scams and prohibited goods. The company described these figures, drawn from internal company documents, as "rough" and declined to provide an alternative figure.[221] [222]

265. This goes to a structural conflict of interest within ad-funded models. Where a platform's income is driven by paid placement and volume, removing high-spend campaigns (even when harmful or illegal) can directly suppress revenue, creating a latent incentive to under-detect or under-enforce against criminal fraudulent advertising. That risk persists even as the Online Safety Act 2023 now imposes legal duties to assess and mitigate illegal-content risks (including fraud), backed by Ofcom enforcement and potential fines. In short, unless compliance is robust, and penalties are credibly enforced, the revenue from paid fraudulent promotions may appear more commercially attractive compared with sporadic or deferred regulatory exposure.

266. The scale of fraud facilitated by online platforms is striking. UK Finance reports that 78% of authorised push payment (APP) fraud originates online, with three-quarters beginning on social media.[223] Yet platforms currently bear no legal liability for victim losses. Voluntary initiatives, such as the Online Fraud Charter, play a useful role in fostering collaboration, but their impact has been limited by the absence of enforcement mechanisms and consistent implementation. As Lord Vaux of Harrowden observed in the House of Lords, technology companies will only act decisively when faced with real financial liability.[224]

267. A targeted failure-to-prevent fraud offence for online platforms would not only close a legal gap but also drive profound cultural change. It would embed fraud prevention into governance structures, incentivise investment in detection technologies, and promote collaboration with law enforcement. It would also rebalance the current system, where financial institutions bear the cost of fraud prevention and victim reimbursement,[225] despite much of the fraud originating elsewhere. In short, such an offence would reflect

---

[221] Reuters, 'Meta is earning a fortune from a deluge of fraudulent ads, documents show', 6 November 2025, [Accessed 6 November 2025].
[222] Wolf, M., 'We have to be able to hold tech platforms accountable for fraud', *Financial Times*, 18 November 2025.
[223] UK Finance, *Annual Fraud Report 2023*, (2023).
[224] Lord Vaux of Harrowden, HL Deb Telecommunications Fraud: Reimbursement of Victims, 14 May 2025, vol. 845.
[225] Payment Systems Regulator, *APP scams reimbursement dashboard for Q2 2025*, [Accessed 20 November 2025]. £112 million has been reimbursed to victims under the mandatory APP fraud reimbursement scheme in the first nine months of the policy (7 October 2024 to 30 June 2025).

the realities of the digital economy and ensure that all actors in the fraud ecosystem are held to a consistent standard of accountability.

268. It is acknowledged that extending a failure-to-prevent fraud offence to online platforms raises legitimate concerns, including technical feasibility, proportionality and jurisdictional enforcement.[226] However, these concerns are not insurmountable. The offence would not impose strict liability, but rather a duty to implement reasonable prevention procedures, tailored to the platform's size, risk profile and operational capacity. This approach mirrors existing corporate liability models and ensures that obligations are both enforceable and proportionate. In this context, the case for reform remains compelling. The following proposal seeks to address the accountability gap identified above and ensure that obligations reflect the realities of the digital economy.

Recommendation 2

Introduce a new corporate criminal offence for providers of regulated user-to-user services (as defined under the Online Safety Act 2023) who fail to prevent fraud on their platforms. This offence would closely mirror the recently introduced 'failure-to-prevent' fraud offence under the Economic Crime and Corporate Transparency Act 2023, which holds large organisations criminally liable if they fail to prevent fraud committed by associated persons for their benefit.

Mandatory Reimbursement

269. While corporate liability is one strand of reform, consumer protection measures, such as mandatory reimbursement, represent another critical dimension of the response to fraud. When considering all actors engaged in the fight against fraud, particular attention must be paid to the financial sector's evolving obligations. On 7 October 2024, the UK implemented a mandatory reimbursement regime for victims of APP fraud, marking a significant shift in consumer protection. The regime is underpinned by Section 72 of the Financial Services and Markets Act 2023,[227] which empowers the Payment Systems Regulator (PSR) to mandate reimbursement for in-scope APP fraud cases executed over the Faster Payments System. It replaces the voluntary Contingent Reimbursement Model Code and applies to consumers, microenterprises and charities.

270. Under the scheme, liability is shared between the sending and receiving payment service providers, who must reimburse 50% of the refund to the sender within five working days. Maximum reimbursement is capped at £85,000 and claims must be made within 13 months of the fraudulent payment. Exceptions include gross negligence by the consumer, complicity, international payments and civil disputes. In the first three months of

[226] Frost, N., *Regulating Big Tech Beyond Borders: Toward a Global Framework*, *Going "global" on big tech regulation*, (2024).
[227] Financial Services and Markets Act 2023, s. 72.

implementation, 86% of APP fraud losses were reimbursed, totalling £27 million returned to victims. Contrary to fears, fraud rates fell, with fewer claims than the same period in 2023.[228] [229] Of those individuals who lost money, 73% were refunded in full, 3% were refunded in part, and 21% were not refunded at all in year to June 2025.[230]

271. In addition to the new rules for mandatory reimbursement, the financial sector has taken forward a number of initiatives in the fight against fraud. Under the Payment Services Regulations 2017, all payment service providers in the UK are required to verify their customers. Confirmation of Payee is a name-checking service, developed by Pay.UK to help prevent APP fraud. The fraud prevention tool alerts customers to an incorrect match between the account details and intended recipient, providing an extra layer of protection for consumers. The PSR has issued several directions to extend the reach of Confirmation of Payee across industry to over 400 firms.[231]

272. More generally, financial services are heavily invested in fraud prevention, including technologies to detect and prevent fraudulent activities. Companies use artificial intelligence (AI) analytics to monitor transactions in real time and detect unusual patterns, such as frequent withdrawals or multiple failed logins, that may indicate fraud. Many banks also run fraud education webinars, have invested in media campaigns, and offer in-app scam alerts.

273. While banks represent the final stage in the fraud chain, it is incontrovertible that a substantial proportion of fraudulent activity originates beyond the financial sector—most notably on social media platforms. The reimbursement regime places liability squarely upon payment service providers yet conspicuously omits those platforms which frequently serve as the initial vector for fraud and, in many cases, derive financial benefit from its proliferation. From the standpoint of equity and legal coherence, it is difficult to justify the exclusion of such platforms from the obligations imposed on financial institutions.

274. Moreover, banks and financial institutions are subject to extensive obligations under the Proceeds of Crime Act 2002 (POCA) and the Money Laundering Regulations 2017 (MLRs). These frameworks require firms to conduct customer due diligence checks, submit suspicious activity reports, and implement risk-based compliance systems to prevent money laundering and terrorist financing. While these regimes are distinct from fraud-specific legislation, they underscore the disproportionate regulatory burden borne by financial institutions compared with other actors in the fraud ecosystem.

---

228 Payment System Regulator, '[The story so far: A snapshot of what we've seen since our APP scams reimbursement requirement went live]', 15 Mary 2025.

229 The Payment Association, '[APP fraud reimbursement: A six-month policy review]', 16 June 2025.

230 Office for National Statistics, *Statistics on Crime in England and Wales*, (2025), Appendix table A1.

231 Payment Systems Regulator, *PS22/3 Extending Confirmation of Payee coverage*, October 2022.

Telecoms Sector

275. Beyond financial services and online platforms, the telecommunications (telecoms) sector illustrates the wider challenge of securing digital infrastructure against exploitation by fraudsters. While telecoms providers are not typically the originators of fraud, their infrastructure is often exploited by criminals to facilitate fraud. Ofcom reported that 82% of UK adults received a suspicious call or message in 2021,[232] and data from UK Finance indicates that 16% of APP fraud cases originate via telecoms channels,[233] accounting for 43% of total fraud losses by value.

276. In response, the Telecommunications Fraud Sector Charter was created and published by the Home Office in 2021.[234] It sets out a nine-point voluntary action plan, with signatories committing to blocking scam calls and smishing texts, sharing intelligence across the sector, and collaborating with banks to strengthen identity verification during mobile contract applications and number porting. A second, expanded charter was published in November 2025, with a focus on closing vulnerabilities such as SIM farms[235] and caller ID spoofing.[236]

277. Ofcom consulted in early 2024 and published updated calling line identification (CLI)[237] guidance on 29 July 2024, requiring providers to block spoofed UK numbers on international calls.[238] These measures came into force on 29 January 2025 and aim to close a significant loophole exploited by fraudsters using overseas or Voice over Internet Protocol-(VoIP-) based services. Ofcom is now considering further steps to extend these protections to UK mobile numbers, addressing vulnerabilities linked to roaming and cloud telephony.

278. In October 2025, Ofcom launched a consultation on new rules to combat mobile messaging scams, recognising that criminals increasingly use SMS and other messaging channels alongside calls and online platforms to target victims. The proposals would require mobile operators and business messaging aggregators to adopt stronger controls to prevent scammers from accessing messaging services and to block fraudulent messages at scale. The consultation closes in January 2026, with final decisions expected in summer 2026.[239]

---

232 Ofcom, '45 million people targeted by scam calls and texts this summer', last updated 16 March 2023.
233 UK Finance, *Fraud remains a major problem as over £1 billion is stolen by criminals in 2023*, press release, (2024), [Accessed 21 October 2025].
234 Home Office, *Fraud sector charter: telecommunications*, (2021).
235 SIM farms are large-scale setups that use hundreds or thousands of SIM cards in devices or modems to send bulk messages or make automated calls, often for fraudulent or spam purposes.
236 Home Office, *UK Telecommunications Fraud Sector Charter*, (2025).
237 Calling line identification allows the person receiving the call to see the caller's number.
238 Ofcom, *CLI Guidance*, (2024).
239 Ofcom, 'Consultation: Combatting Mobile Messaging Scams', 29 October 2025.

279. While telecoms providers are increasingly required to block fraudulent calls, stakeholders noted that they must balance fraud prevention with legitimate communication needs. Calls often pass through multiple networks or originate from cloud-based platforms, making it difficult to verify their authenticity. Under Ofcom's CLI guidance, providers must ensure that blocked calls are based on valid, dialable CLI data, which introduces a risk of inadvertently disrupting genuine communication.

280. Industry bodies such as TechUK raised concerns to this Review about the lack of a centralised repository for number tracing, which hampers efforts to identify and block fraudulent traffic. Providers have also called for clearer Know Your Customer (KYC) obligations before issuing numbers, to prevent misuse by criminal actors.

281. Representatives from the telecommunications sector informed this Review of other measures being implemented to reduce the risk of their services being exploited for fraudulent purposes. One such initiative is Scam Signal, a cross-industry collaboration between mobile network operators and banks, coordinated by UK Finance and the Global System for Mobile Communications Association.[240] It uses real-time data to detect and prevent APP fraud. Early pilots have shown a 30% improvement in scam detection.

282. As with other sectors, the industry is deploying AI tools to combat fraud, and since 2023 over 1 billion scam messages have been blocked by mobile operators.[241] I also heard that AI tools are being used to flag and label suspicious calls to users. However, this has not been without criticism; as Lord Vaux pointed out in his speech to Parliament, some companies have introduced these as paid-for services, raising questions about access to fraud prevention[242] and motivations for tackling the issue.

283. UK telecoms providers are making progress in fraud prevention, but further investment, regulatory clarity and cross-sector collaboration are essential. As fraud increasingly migrates across digital infrastructure, the sector must continue to play an active role in protecting consumers and supporting enforcement efforts.

Anti-Fraud Levy

284. Finally, attention must be given to the question of financial responsibility. If fraud prevention is to be systemic, all actors whose platforms are exploited must contribute proportionately to enforcement and victim support. This Review received compelling and consistent evidence from across the criminal justice system, financial services, consumer protection bodies and other stakeholders. There was broad consensus, excluding the online sector, that industries whose infrastructure facilitates fraud should bear proportionate responsibility. This includes online platforms that host paid advertisements

[240] GSMA and UK Finance, 'Mobile and Banking Industries Join Forces to Fight Fraud', press release, 5 November 2024.
[241] Mobile UK, 'UK Mobile Industry Blocks One Billion Scam Messages', 6 November 2024.
[242] Lord Vaux of Harrowden, HL Deb Telecommunications Fraud: Reimbursement of Victims, 14 May 2025, vol. 845.

for scams, enable impersonation fraud and facilitate phishing schemes. These harms are not incidental but stem from systemic vulnerabilities in platform design and monetisation models.

285. Platforms argue that they are unfairly portrayed as indifferent to harmful content, asserting that it is in their commercial interest to remove such material. They also cite the difficulty of identifying 'pre-fraudulent' content. While these concerns are not without merit, they do not absolve platforms of responsibility. The difficulty of detection cannot justify inadequate action, particularly when victims suffer severe financial and non-financial harm, and platforms continue to profit from engagement metrics linked to such content.

286. These concerns are borne out in practice. It takes only minutes of browsing a social media feed to encounter suspicious ads, fake profiles or misleading investment opportunities. The scale and visibility of fraudulent content suggest that platforms are not passive conduits but central actors in its propagation.

287. While the Online Safety Act 2023 introduces duties of care, it does not address the commercial incentives that drive online fraud. Platforms that profit from fraudulent advertising face no direct financial liability for victim losses or profits from fraudulent advertising. This misalignment must be corrected if meaningful change is to be achieved.

288. The Economic Crime Levy,[243] introduced via the Finance Act 2022, requires anti-money laundering (AML) regulated entities to contribute to anti-money laundering efforts. Levy proceeds are ringfenced for enforcement and prevention initiatives, including funding intelligence teams and technology upgrades. Analogous models exist, such as the Climate Change Levy,[244] which internalises environmental costs and incentivises cleaner practices.

289. Given the scale and impact of fraud, and in the interest of fairness, online platforms should also contribute financially. Tackling fraud requires a level playing field, where all actors whose infrastructure is exploited share responsibility. This raises the question of whether technology companies are contributing proportionately, and whether an anti-fraud levy should be introduced to support prevention, enforcement and victim support.

290. I do recognise that some companies are taking meaningful steps to design fraud out of their platforms. For example, major dating app providers are introducing enhanced identity verification, AI-driven scam detection, and proactive user education campaigns.[245] These efforts demonstrate that fraud prevention can be embedded into platform design without undermining user experience or commercial viability. A levy would not diminish or penalise such initiatives; rather, it would complement them by ensuring that all actors

---

[243] HM Revenue and Customs, *Economic Crime (Anti-Money Laundering) Levy*, (2021).
[244] HM Revenue and Customs, HM Treasury and Environment Agency, *Climate Change Levy: detailed information*, (2025).
[245] Match Group, 'Tinder to Expand Facial Verification Feature Across the U.S., Setting a New Standard for Dating Safety', press release, 22 October 2025.

contribute proportionately to systemic prevention and victim support. Those investing in robust safeguards would remain well positioned to benefit from a fairer, securer digital ecosystem.

291. A levy could be proportionate to advertising revenue or user-base size, with funds earmarked for enforcement, awareness campaigns and victim support. It could be overseen by Ofcom, with a sunset clause for its reduction or removal if platforms demonstrate measurable improvements in fraud prevention and cooperation with law enforcement.

Recommendation 3

Introduce an anti-fraud levy on digital and communications infrastructure providers, including social media platforms, online service providers, and other intermediaries that host or facilitate fraudulent activity. The levy would aim to distribute the financial burden of economic crime more equitably across all stakeholders whose platforms are exploited for fraud. It would be administered by Ofcom, with a sunset clause allowing for its reduction or removal if measurable improvements in fraud prevention, detection, and cooperation with law enforcement are demonstrated.

292. Funds raised through the levy could be reinvested to create a **virtuous cycle**—supporting law enforcement, funding public education campaigns, and enabling technological innovation in fraud detection. This would not only enhance consumer protection but also incentivise platforms to embed fraud prevention into their core governance and operational models.

293. In conclusion, the UK's anti-fraud legislative trajectory reflects a growing recognition that fraud cannot be addressed solely through individual liability. Corporate responsibility, regulatory duties and consumer protection measures form essential components of a multi-layered strategy. Yet gaps remain—particularly around online platforms and cross-sector accountability.

294. Real progress depends on preventing and disrupting fraud upstream, before victims are exposed, through decisive action by technology companies and other actors. This requires a shift from a reactive model, leaving the justice system being overwhelmed, to a proactive, collaborative approach targeting the infrastructure of fraud. Voluntary agreements have a role, but if major actors fail to grip this escalating threat, more prescriptive measures may be unavoidable. The imperative is clear: fraud must be designed out of systems, not merely prosecuted after the harm is done.

7. Emerging Threats and Satellite Offences

295. The resilience of the Fraud Act 2006 must be tested not only against traditional forms of deception but also against the evolving threat landscape. Fraud is no longer confined to financial misrepresentation or corporate dishonesty; it now encompasses a spectrum of conduct enabled by digital platforms, artificial intelligence (AI) and identity manipulation. These developments raise pressing questions about the adequacy of existing legal frameworks and the need for targeted reform.

296. This chapter examines five distinct but interrelated areas of concern:

a. Romance fraud, which exploits emotional vulnerability for financial gain.

b. AI-enabled fraud, which automates deception at scale.

c. Identity theft and deed poll abuse, which facilitate impersonation and concealment.

d. Money laundering and muling, which enables the laundering of fraud proceeds.

e. The case for ancillary offences to support proportionate enforcement.

297. Each section considers whether the Fraud Act remains fit for purpose, and where legislative or procedural reform may be warranted. The analysis draws on recent case law, sentencing guidance and international models, with a view to strengthening the criminal justice response to modern fraudulent conduct.

Romance Fraud

298. Romance fraud represents a particularly insidious form of deception, exploiting emotional vulnerability for financial gain. Enabled by the proliferation of digital platforms, particularly dating apps and social media, this offence is marked by intense psychological manipulation, often leaving victims not only financially harmed but emotionally devastated.[246]

299. Perpetrators construct false identities using deepfake technology, synthetic profiles, and scripted interactions to build trust rapidly. Victims are frequently targeted across borders, complicating jurisdictional enforcement.[247] While the Fraud Act 2006 captures such

[246] Whitty, M. T. and Buchanan, T., The online dating romance scam: The psychological impact on victims – both financial and non-financial, *Criminology & Criminal Justice*, vol. 16, no. 2, 2016, pp. 176–194.
[247] WIRED, The Real-Time Video Deepfake Romance Have Arrived, 18 April 2024, [Accessed 1 November 2025].

conduct under Sections 2 and 4, the emotional harm inflicted often exceeds the financial loss, raising questions about whether the current legal framework sufficiently reflects the gravity of the offence.

300. Sentencing practice has begun to evolve. In 2024, the Sentencing Council revised its guidelines to ensure emotional and psychological harm is properly recognised, even where pecuniary loss is minimal.[248] This shift is welcome, but further reform may be needed to ensure that the unique harm profile of romance fraud is consistently addressed.

Case Study – Dating apps and websites

In April 2025, five individuals were convicted at Guildford Crown Court for their roles in a complex romance fraud and money laundering scheme which targeted 40 confirmed victims (with up to 99 suspected). The criminals created fake profiles and fictional biographies on dating websites to manipulate victims into thinking they were in genuine relationships. The victims, many of whom were recently divorced or widowed, were then asked for money to cover fabricated emergencies, such as failed business trips and stolen wallets. The perpetrators laundered the stolen funds through bank accounts, estimated to total £3.25 million.[249]

Whilst romance fraud is often stereotyped as being perpetuated by men, the reality is more complex, and women, too, can be perpetrators. Between 2022 and 2025, a 37-year-old woman used fake dating profiles and social media accounts to defraud three men out of almost £12,000. She fabricated stories to elicit sympathy and financial support from her victims, who believed they were helping someone in genuine need. She was arrested and charged with three counts of fraud by false representation, and admitted guilt, receiving a two-year suspended sentence.[250]

301. Case law supports this approach. In *R v Alexander*,[251] the Court of Appeal upheld a custodial sentence despite the absence of financial loss, recognising the seriousness of emotional exploitation. The judgment referenced *R v Falder* [2018] EWCA Crim 2514, affirming that psychological damage may be as serious as financial harm.

302. While the creation of a bespoke offence may not be necessary, there is merit in considering romance fraud as an aggravating factor in sentencing, particularly where deception is sustained and emotionally coercive. The cross-border nature of many such

---

248 Sentencing Council, *Miscellaneous amendments to sentencing guidelines: Response to third annual consultation*, (2024).
249 Crown Prosecution Service, 'Money launderers used romance fraud to scam 40 victims out of an estimated £3.25 million', press release, 4 April 2025.
250 Essex Police, 'Harlow: Romance fraud victim thanks officer', 11 August 2025.
251 *R v Alexander* [2022] EWCA Crim 1868.

offences also underscores the need for enhanced international cooperation and digital evidence-sharing protocols, to which I shall return to later.[252]

Case Study – *R v Alexander* [2022]

In R *v Alexander,* the defendant was convicted under the Fraud Act 2006 for deceiving a victim into sending intimate photographs through fake social media profiles. Although the fraud did not result in financial loss, the court recognised the significant emotional and psychological harm caused. The sentencing judge imposed two years and 9 months' imprisonment, reflecting the seriousness of the manipulation and breach of trust.

On appeal, the defendant argued that the absence of financial harm should have reduced the sentence. However, the Court of Appeal upheld the original sentence, The court referenced *R v Falder* [2018] EWCA Crim 2514 to support its reasoning, highlighting that emotional and psychological damage can be as serious as financial loss, particularly when victims are manipulated or exploited.[253]

AI-Enabled Fraud

303. Romance fraud exploits emotional vulnerability, often through digital communication, and AI enables similar deception—albeit now with greater scale, speed and sophistication. The transition from human-led manipulation to machine-assisted fraud marks a significant evolution in the threat landscape.

304. AI tools are now being deployed to impersonate, deceive, and defraud with minimal human input, raising new challenges for enforcement and prosecution. Deepfakes,[254] synthetic voices and impersonation tools are increasingly being deployed to deceive victims, often with content indistinguishable from reality. In a July interview with the US Federal Reserve, Sam Altman the CEO of OpenAI, said that AI has already defeated many bank verification systems and warned of a "significant, impending fraud crisis".[255]

305. In light of the emergence of this novel technology, it is necessary to assess whether the current legal framework, most notably the Fraud Act 2006, remains sufficiently robust to address this new and evolving form of criminal conduct.

306. Although the Fraud Act 2006 was not drafted with AI in mind, its provisions, particularly section 6, are sufficiently broad to accommodate the prosecution of AI-enabled offending. Section 6 criminalises possession or control of any 'article' for use in the course of or in connection with fraud. The statutory definition of 'article' under section 8

[252] See chapter 'International'.
[253] *R v Alexander* [2022] EWCA Crim 1868.
[254] Deepfake – Computer generated media that convincingly mimic a person's appearance or voice.
[255] Bloomberg Television, 'Sam Altman on How AI Could Impact Banking', video, streamed live on 22 July 2025.

explicitly includes programs and data held in electronic form, thereby capturing AI models, scripts, bots and datasets used to facilitate fraud. The offence is not limited to tools used in the execution of fraud, but also includes those used in preparation, concealment or facilitation.

307. Case law has affirmed the breadth of this provision. In *R v Smith (Andrew)*,[256] the Court of Appeal held that a falsified document created post-fraud was still an article used 'in connection with' the offence. Similarly, *R v Hana Rasoul*[257] confirmed that control may be established even where the article is not physically possessed. The requirement is not for a specific fraud, but a general intention to use the article in connection with any fraud, making the provision particularly apt for AI tools designed for broad deployment across multiple schemes.

Case Study – Evolution of 'Hi Mum' Fraud

In 2025, UK parents continued to receive WhatsApp messages from unknown numbers claiming to be their children who had lost their phones and needed urgent financial help. Though this is not a new fraud method, reports have been made to Action Fraud of parents transferring funds after receiving a voice note that sounded exactly like their child. Criminals had scraped voice clips from social media and used AI voice cloning to generate a convincing message. Experts warn that this same technology is now being used not only to defraud individuals but also to bypass bank security systems that rely on voice authentication. In a BBC investigation, a journalist successfully accessed her own bank accounts using an AI-generated clone of her voice.[258] [259] [260]

Case Study – AI Bot Romance Scam Victim

A UK man attempted to transfer £10,000 to someone he believed was his online girlfriend. Despite warnings from Lloyds Bank and police involvement, he insisted she was real, describing her as a chef who worked on an oil ship and had just flown from Texas to Paris. The interaction showed all the hallmarks of an AI-powered chatbot: scripted replies, emotional manipulation, and evasiveness. The victim was unable to speak to her directly yet remained convinced of her existence—suggesting he may have been conversing with a bot programmed to simulate romantic engagement.[261]

---

256 *R v Smith (Andrew)* [2020] EWCA Crim 38.
257 *R v Hana Rasoul* [2012] EWCA Crim 3080.
258 BBC News, 'BBC presenter's mother lost £47k in 'text mum' scam', 1 April 2024.
259 The Independent, *WhatsApp scam known as 'hi mum' evolving at 'breakneck speed', expert warns*, (2025).
260 Vahl, S., 'Cloned customer voice beats bank security checks', BBC News, 28 November 2024.
261 Williams, E., '"I bet you £20k she's real": Transcript reveals romance scam victim arguing with bank employee', *The Telegraph* 17 September 2025.

308. Section 6 offences are also eligible for Deferred Prosecution Agreements (DPAs) under Schedule 17 of the Crime and Courts Act 2013, making it applicable to corporate entities involved in the development or deployment of fraud-enabling technology. The Sentencing Council guidelines provide a structured framework for assessing culpability and harm, though further consideration may be needed to ensure they adequately reflect the scale and sophistication of AI-driven deception.

309. The Independent Reviewer of Terrorism Legislation, Jonathan Hall KC, has already raised concerns about the threat posed by AI and discusses new legal responses, including a possession offence modelled on section 7.[262] This underscores the relevance and adaptability of the provision, and its potential as a template for future legislative reform. As criminals increasingly rely on easily accessible and effective AI-powered tools to commit fraud, prosecutors may in turn pivot to focus on charges under section 6 and 7 of the Fraud Act.[263]

310. I have heard reports that existing criminal law is generally fit to prosecute individuals who use AI to commit criminal offences; however, there is a potential legislative gap relating to conspiracy with AI. Under current law, a person can only be convicted of conspiracy if they conspire with another human, as criminal conspiracy requires an agreement by two or more *persons* to carry out a criminal act. As an AI tool is not a legal person, one cannot conspire with it and therefore the law does not currently allow for a conviction where a human unknowingly conspires with an AI tool. Addressing this gap would require amending both the statutory offence of conspiracy and the common law offence of conspiracy to defraud. I understand the Government is considering the merits of a possible amendment on this matter.

311. Importantly, the essence of fraud remains rooted in deception and dishonesty. The tools used to commit the fraud are important but secondary. AI may be incidental to the offence, but where it is deliberately deployed to deceive, the existing legal principles remain applicable. The Fraud Act is, at present, well placed to address AI-enabled fraud. However, as technology evolves, particularly with the emergence of autonomous systems and bots, ongoing review will be essential to ensure the law remains fit for purpose.

<u>Satellite Offences</u>

312. While the Fraud Act 2006 is a versatile instrument for prosecuting fraudulent conduct, its practical application is not without limitations. The triable-either-way nature of the offences often necessitates complex and resource-intensive proceedings. The average time from receipt at the Crown Court to completion, for a fraud case, remains substantial: 442 days. This is contributing to delays that disincentivise investigators and prosecutors

[262] Home Office, *The Terrorism Acts in 2023: report of the Independent Reviewer of Terrorism Legislation*, (2025), paragraph 98.
[263] Ministry of Justice, *Outcomes by offence tool*, Criminal court statistics quarterly: June 2025 publication.

from pursuing certain cases. These delays also discourage early guilty pleas, compounding inefficiencies and undermining the swift delivery of justice.

313. In my view, there is a compelling case for the introduction of a suite of ancillary or 'fraud-adjacent' satellite offences. These would not supplant the Fraud Act but rather complement it, providing prosecutors with proportionate tools to address enabling or peripheral conduct. This approach mirrors other areas of criminal law, where core offences are supported by satellite provisions. For example, the Offences Against the Person Act is supplemented by targeted offences such as coercive control, stalking, and child cruelty, each isolating specific forms of harm that may not be adequately captured by general provisions.

314. Ancillary offences in the fraud context would serve a similar purpose. They would isolate and criminalise conduct that facilitates or accompanies fraud, such as reckless facilitation, impersonation for unlawful purposes, or the use of identity mechanisms to obscure criminal history. These behaviours, while not always amounting to full-scale fraud, are damaging in their own right and erode public confidence in the integrity of financial and digital systems.

315. I propose that such offences be designated as summary-only, enabling resolution in the magistrates' court. This would allow for:

a. Swifter trials, avoiding the delays and costs of Crown Court proceedings.

b. Proportionate enforcement, particularly for low-level or first-time offending.

c. Clear signalling, that enabling conduct is criminal and will be addressed.

d. System efficiency, by diverting cases from the Crown Court backlog.[264]

e. Cost-effectiveness, reducing the financial burden on the justice system.

316. Strengthening the enforcement toolkit in this way would allow law enforcement to respond flexibly across the fraud spectrum. It would also reinforce the deterrent effect of fraud enforcement, ensuring that even peripheral or preparatory conduct is met with a legal response. In doing so, it would enhance public confidence and better reflect the realities of modern fraudulent behaviour.

Identity Theft

317. The absence of a standalone offence for identity theft has drawn increasing attention. Identity theft involves the unauthorised acquisition of personal information, such as name, date of birth, and address. While it often serves as a precursor to fraud, it is not

[264] Ministry of Justice, *Independent Review of the Criminal Courts: Part 1.* (2025).

considered a recordable crime unless the stolen identity is used to obtain financial gain, at which point it becomes identity fraud. Stolen identities are often used to open bank accounts, commit benefit or credit card fraud, and ultimately facilitate serious and organised crime. Increasingly, and as discussed,[265] criminals are acquiring personal data online through social engineering and data breaches. According to Cifas, identity fraud was the most reported fraud type in 2024, with over 249,000 cases, accounting for 59% of all fraud filings.[266]

318. Much has been said about not having a separate offence of identity theft, including the House of Lords Fraud Act 2006 and Digital Fraud Committee report, titled *Fighting Fraud: Breaking the Chain*, which recognised identity theft as a "fundamental component of fraud", yet it remains out of scope of criminal offences.[267] The committee recommended consulting on creating a specific criminal offence of identity theft or, alternatively, considering identity theft as a serious aggravating factor for fraud.[268] However, UK law does not currently treat identity theft as a standalone offence. Instead, it is addressed through a combination of existing legislation:

a. Computer Misuse Act 1990 – Criminalises unauthorised access to computer systems, including the theft and sale of personal data.

b. Fraud Act 2006 – Covers the use of personal data to commit fraud, including the creation and distribution of false identities.

c. Identity Documents Act 2010 – Criminalises the use of false identity documents with intent to misrepresent another person's identity.

d. Data Protection Act 2018 (GDPR) – Sets standards for handling personal data; breaches can result in prosecution.

319. Identity theft is treated as a gateway to fraud rather than a crime in its own right. This gap feels out of step with the experience of victims, especially those who have to endure arduous steps to try and repair their identity. In their report *Who Do You Think You Are: Recommendations on the Future Response to Large-Scale Identity Fraud*, the Royal United Services Institute (RUSI) and Cifas highlight the lack of a standalone offence for identity theft, creating ambiguity in enforcement and prosecution.[269] They also recommend a review of the law on identity theft to ensure it provides an adequate deterrent.

320. The theft of someone's identity is uniquely harmful. It involves the unauthorised appropriation of something deeply personal, the essence of who a person is. Victims often feel powerless. The consequences of identity theft extend beyond emotional distress. Victims may face long-term financial exclusion, including difficulty securing loans,

---

265 See chapter 'Enablers and Connected Criminality'.
266 Cifas, *This is Fraudscape 2025*, (2025).
267 House of Lords Fraud Act 2006 and Digital Fraud Committee, Fighting Fraud: Breaking the Chain, HL 87, (2022).
268 Ibid.
269 Westmore, K. and Wood, H. Recommendations on the Future Response to Large-Scale Identity Fraud, Royal United Services Institute, (2024),.

mortgages, or employment due to damaged credit records.[270] [271] These impacts are not incidental, but form part of the core harm caused by impersonation.

321. Crucially, it undermines personal autonomy: the ability of an individual to control how they are represented, recognised, and engaged with in both digital and physical domains. The erosion of this autonomy is not merely incidental, it is central to the harm caused by identity theft.

Case Study – Identity Theft and the Unrecognised Victim

A 38-year-old man from Belfast had his identity stolen and used to fraudulently open mobile phone contracts, resulting in debts of nearly £3,000. Although he did not lose money directly, the fraud had a profound impact on his life. His credit rating deteriorated, he received weekly enforcement letters, and his details were passed to debt collectors. He described the experience as "very stressful" and "emotionally distressing", noting that the damage to his credit file jeopardised future financial applications.

Despite the harm suffered, he was not recognised as the legal victim of fraud under the Fraud Act 2006. The mobile provider was considered the victim, as it incurred the financial loss. The man, whose identity was misused, was treated as a victim of identity theft—a status that carries limited legal recognition and protection.[272]

322. Under current law, when a fraud is committed using stolen identity, the individual whose identity is misused is not recognised as the legal victim of the fraud unless they themselves suffer financial loss. The victim, for the purposes of the Fraud Act 2006, is the person whose assets are targeted. This doctrinal distinction fails to reflect the experience of those whose identities are exploited to facilitate criminal conduct. It also risks marginalising the harm suffered by individuals, who must navigate the consequences of impersonation, reputational damage and administrative burden.

323. In my view, this gap in recognition and protection warrants legislative reform. I propose the creation of a standalone offence: the unauthorised acquisition and use of sensitive personal information, such as names, addresses, national insurance numbers or biometric data, for the purpose of impersonating another individual and carrying out a fraud. Such an offence would isolate and criminalise the act of identity theft itself, rather than treating it merely as a gateway to fraud. It would also ensure that those whose identities are

[270] Ibid page 8.
[271] Information Commissioner's Office, 'Identity theft', [Accessed 30 October 2025].
[272] Stewart, A., Identity theft: Belfast man speaks of stress after scam, BBC News, 18 February 2024).

misused are properly recognised as victims under the law, and that the violation of personal autonomy is treated with the seriousness it deserves.

Recommendation 4

Introduce a specific summary-only offence of identity-based impersonation, defined as the use of another person's personal details or identity for the purpose of committing fraud.

324. In addition to criminal sanctions being imposed on the perpetrators of identity theft, victims should be empowered to seek compensation orders. Where identity theft results from a data breach or negligent handling of personal data, victims may pursue civil claims under the Data Protection Act 2018 and UK GDPR. These claims can cover both material losses (e.g. financial harm) and non-material damage (e.g. distress). A standalone offence would strengthen the legal basis for such claims, allowing courts to more readily recognise the harm suffered and award appropriate redress.

Deed Poll Abuse

325. While identity theft typically involves the unauthorised acquisition and use of personal data, criminals are also exploiting legal mechanisms to assume or obscure identities. One such method is the abuse of the deed poll system, which allows individuals to legally change their name. This process is being used not just to impersonate others but to construct new fraudulent identities or conceal criminal histories, making it a powerful enabler of identity-based fraud.

326. Under common law, individuals over the age of 16 in the UK have the right to change their name at any time using the deed poll process.[273] This right is protected by common law and applies regardless of personal circumstances, including criminal history, though there are reporting obligations for some offenders. The guidance notes that an individual cannot change their name if they are doing so for a fraudulent or unlawful purposes, though this exemption has no legal standing.[274]

327. There are two types of deed poll: unenrolled, which is created privately and creates no public record, and enrolled, which is recorded at the Royal Courts of Justice and published in *The Gazette*. The National Archives estimate that less than 1% of changes by deed poll are enrolled.[275] There is no central repository of name changes nor any requirement to

[273] UK Government, 'Change your name by deed poll', [Accessed 20 September 2025].
[274] National Archives, 'Changes of names', [Accessed 20 September 2025].
[275] Ibid.

notify Government bodies. This lack of oversight makes it challenging to track individuals who have used multiple identities.

328. The review has heard evidence that organised crime groups are utilising deed poll name changes to facilitate fraud. This includes taking over accounts, creating mule accounts, and carrying out property fraud. Once the name change is confirmed, passports can be obtained, allowing criminals to use this as proof of identity to open or modify bank accounts, bypassing anti-fraud checks implemented by financial institutions.

329. A notable case from 2017 involved two women who used a deed poll name change to impersonate an elderly property owner of a £1.2-million house in Kensington. They secured a bridging loan against the property, which was later identified as fraudulent by HM Land Registry. Although the property owner did not lose their home, the loan company suffered financial loss, and both women were convicted and sentenced to prison.[276]

330. In response to growing concerns of offenders disguising their history, the Crime and Policing Bill, introduced on 25 February 2025 proposed new restrictions on the ability of sexual offenders to change their name.[277] This included advance notification of at least seven days of any intended name change, and requirements for prior approval on official documents. The police will also be able to refuse permission entirely if they believe the name change poses a risk to public safety.

331. There are of course a range of situations, including marriage, and other scenarios requiring the protection of children and adults from abusers, where name changes are necessary, and the right to change one's name for legitimate reasons must be preserved. However, it is clear the deed poll system continues to be abused by criminals who use it to disappear, avoid detection and continue their offending. It is in effect a significant loophole.

332. To this point, I recommend introducing a targeted criminal offence to address the misuse of the deed poll process for fraudulent purposes. This would be a moderate but important step in signalling the intent of law enforcement to tackle such behaviour. More extensive reforms, such as a fundamental review of the deed poll system, fall outside the scope of this review. However, without changes to policy on formal identity documentation, significant vulnerabilities will persist. Below, I outline one potential approach for consideration.

[276] Prasad, J., 'High-profile case shows how property fraud can happen', HM Land Registry blog, 16 January 2017, [Accessed 25 September 2025].
[277] House of Commons, *Crime and Policing Bill (Tenth sitting) - Hansard - UK Parliament*, 24 April 2025.

> **Recommendation 5**
>
> Create a summary-only offence for Deed Poll Abuse—changing one's name through the deed poll process with the intent to commit a fraud.

Digital Identity Verification

333. The abuse of the deed poll system is symptomatic of a wider vulnerability in the UK's identity infrastructure. Whether through legal name changes, synthetic identities, or impersonation using stolen credentials, the ability to assume or obscure identity remains a powerful enabler of fraud. In response, there is renewed interest in the potential of digital identity systems to strengthen verification, reduce impersonation risk and improve fraud resilience.

334. The UK Government's proposed framework for Digital Verification Services (DVS), set out in Part 2 of the Data (Use and Access) Act, aims to establish a statutory trust framework for digital identity providers. The legislation mandates certification, oversight and public registration of DVS providers, with the goal of enabling digital identities to be used with the same confidence as physical documents.[278]

335. Properly implemented, digital identity systems could enhance onboarding processes across financial services, flag anomalies in real time, and reduce reliance on easily forged documents. The Centre for Finance, Innovation and Technology (CFIT) estimates that a secure, scalable DVS could unlock £1.8 billion in economic value by 2031 and reduce fraud losses by at least £3 billion.[279] Integration with biometric verification and smart data protocols may further strengthen fraud prevention efforts. More recently, the Government formally announced the rollout of a new digital ID scheme, designed to simplify access to public and private services and strengthen identity assurance across sectors.[280]

336. However, the limitations are significant and must be acknowledged. Fraudsters rarely use their true identities and are adept at producing convincing forgeries—including fake passports, driving licences and, increasingly, synthetic digital identities. A digital ID system, if not underpinned by rigorous verification and anti-tampering safeguards, could be vulnerable to similar exploitation.

[278] Data (Use and Access) Act 2025, Part 2, Sections 27–28.
[279] Centre for Finance, Innovation and Technology (CFIT), 'CFIT publishes Digital Company ID plan to slash fraud, saving UK businesses billions annually', (2025).
[280] Department for Science, Innovation and Technology, *Digital ID scheme: explainer,* (2025).

337. There are also civil liberties concerns. Centralised identity systems raise questions around surveillance, data retention, and exclusion, particularly for individuals without access to digital infrastructure. The potential for misuse or mission creep, where identity systems are repurposed for unrelated enforcement or profiling, must be guarded against. These risks are not hypothetical; they are grounded in historical experience and contemporary privacy jurisprudence.

338. In conclusion, while digital identity cards are not a panacea, they may offer incremental value in the fight against fraud, particularly when deployed as part of a multi-layered identity assurance ecosystem. Alternatives such as Government-supported third-party verification services, enhanced deed poll and impersonation offences, and sector-specific identity protocols may offer similar benefits, with fewer civil liberty concerns. Nonetheless, given the evolving threat landscape and the increasing sophistication of fraud techniques, it would be prudent to explore the potential of digital identification, ensuring that any deployment is proportionate, privacy-respecting, and demonstrably effective.

Money Laundering

339. Finally, I turn to low-level money laundering, sometimes termed ‘money muling’, which is a quintessential criminal-enabling practice. It represents the operational end-point of many frauds discussed earlier in this chapter, whether through stolen credentials, manipulated digital identities, or name changes via deed poll. Where identity theft facilitates access, and digital impersonation enables deception, money muling completes the cycle by laundering the proceeds. It is the mechanism by which illicit funds are moved, obscured and legitimised, often through the exploitation of vulnerable individuals and the banking system itself.

340. The process involves the rapid movement of illicit funds through a network of ‘mule’ accounts, often across borders. The National Crime Agency (NCA) estimates that over £10 billion is laundered annually through such activity. In 2022 alone, UK banks identified over 39,000 accounts exhibiting behaviour indicative of money muling,[281] with over 16,000 cases indicative of money-muling activity reported in the first half of 2025.

341. But, as Professor Michael Levi points out in *Perceptions of Money Laundering and of the Legitimacy of Anti-Money Laundering*,[282] the risk of a criminal record for money laundering, and denial of financial services facilities through Cifas markers on suspected money mules

281 Home Office, Biggest ever crackdown on money mules in the UK, news story, 1 March 2024.
282 Cifas, *This is Fraudscape 2025*, (2025).

is rare.[283] It is therefore not surprising that, in a recent Cifas survey, one in five people thought money muling was legal.[284]

342. Money muling typically involves an individual (the 'mule') transferring or receiving criminal proceeds on behalf of others, often using their personal bank account.[285] This may include allowing access to their account, withdrawing and handing over cash, or facilitating cryptocurrency transactions. While many mules are complicit, others, particularly young people and vulnerable adults, may be coerced or manipulated into participation.[286] It is estimated that 23% of money mules are under 21, and 65% are under 30.[287]

343. Although money muling is prosecuted under money laundering legislation, it is frequently the final stage in a fraud lifecycle. The funds being transferred are often the proceeds of scams, deception or digital impersonation. In this sense, muling is not merely adjacent to fraud, it is integral to its execution and concealment.

344. Currently, the principal enforcement mechanism is prosecution under the Proceeds of Crime Act 2002 (POCA), including section 327 (concealing or transferring criminal property), section 328 (facilitating acquisition or use), and section 329 (possession of criminal property). These offences carry a maximum sentence of 14 years' imprisonment or an unlimited fine. However, this approach may be disproportionate for low-level or first-time offenders, particularly where intent is difficult to prove or coercion is suspected.

345. In April 2024, the Crown Prosecution Service (CPS) updated its guidance on money laundering, recognising the role of 'mule herders' in exploiting vulnerable individuals.[288] The guidance also endorsed the potential use of Economic Cease & Desist Notices as an early non-prosecutorial intervention. These notices serve as formal warnings and are a valuable out-of-court disposal mechanism, particularly where prosecution is not in the public interest, and in cases of limited culpability and harm involving low-level money mules rather than organisers. Decisions on issuing such notices rest with the investigating force or officer, who must justify their use in each case. Prior service of a Cease & Desist Notice may later provide evidence that a suspect knew property was derived from criminal proceeds.

346. To build on this, I propose an adaptable enforcement model for low-level money mule offending. This would ensure proportionality, safeguard vulnerable individuals, and reduce pressure on the criminal justice system.

---

283 Levi, M., 'Perceptions of Money Laundering and of the Legitimacy of Anti-Money Laundering', paper presented at the Third International Research Conference On Empirical Approaches To Anti-Money Laundering, Nassau, the Bahamas, page 15.
284 Cifas, *Fraud Behaviours Survey 2024*, [Accessed 22 September 2025].
285 Home Office, *Money mule and financial exploitation action plan*, (2024).
286 The Children's Society, *Moving money*, (2025).
287 Home Office, 'Biggest ever crackdown on money mules in the UK', news story, 1 March 2024, [Accessed 22 September 2025].
288 Crown Prosecution Service, *Money Laundering Offences*, (2024).

a. **First instance** – Where an individual is suspected of money muling for the first time and the value of money moved is small, then law enforcement should issue an Economic Cease & Desist Notice. If the individual is assessed as vulnerable or potentially coerced, a referral should also be made to an appropriate safeguarding body.

b. **Second instance** – If the same individual is subsequently found to be involved in money muling, a financial penalty should be considered. This may take the form of a fixed penalty notice or a conditional caution with a financial element, depending on the circumstances.

c. **Third instance** – Where a non-vulnerable individual continues to engage in money muling despite prior warnings and penalties, prosecution may be appropriate. In such cases, a new summary-only offence, tailored to low-level money mule conduct, would provide a more proportionate alternative to full-scale money laundering charges under POCA.

347. Crucially, a tailored enforcement model would enable officers to isolate and address the enabling conduct of money muling without resorting to full-scale prosecution under POCA, a legislative sledgehammer ill-suited to cracking a focused nut. It would allow for a proportionate and flexible response to varying levels of culpability, preserving the option of full prosecution for serious or repeat offending, while diverting low-level or vulnerable individuals into appropriate support pathways.

348. This approach reflects the reality that many first-time mules are not career criminals, but individuals who have failed to exercise due care or have been manipulated into participation. It also recognises the long-term consequences of a criminal record, which can severely impact access to education, employment and financial services. In this context, a structured model offers not only procedural efficiency but a more humane and targeted response to a growing enabler of fraud.

349. Current offences under POCA require proof that the defendant knew or suspected the money was criminal property. A lower-intent threshold, accompanied by a lower penalty, would better reflect cases where individuals should have known, or failed to exercise due care, rather than those where defendants acted with clear criminal intent.

350. International models offer useful precedent. In Singapore, for example, amendments to the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act were tabled in April 2025 to introduce new offences for 'rash or negligent' money laundering.[289] These reforms aim to lower the threshold for prosecution and address the evidential challenges of proving intent in mule cases. The UK should consider similar

[289] Singapore Police Force, *CDSA and CMA Bill Amendments*, (2025), [Accessed 22 September 2025].

innovations to ensure its enforcement toolkit remains fit for purpose in the face of evolving threats.

351. Such an approach would signal that money muling is not a harmless or low-risk activity. The current binary system, prosecution or no action, fails to deter those who perceive money muling to be a minor offence. A structured response, beginning with formal warnings and escalating to penalties and prosecution, may reinforce the seriousness of the conduct and cause individuals to reconsider participation. It would also allow law enforcement to resolve cases more efficiently, freeing up capacity for complex investigations and greater focus on the organised minds behind criminal networks.

352. Importantly, the effectiveness of a multi-pronged penalty model is strengthened when paired with targeted education and awareness initiatives—particularly for children and young adults entering financial autonomy. As discussed later,[290] early intervention for children, through financial literacy and fraud prevention education, is essential to reducing the appeal and perceived legitimacy of money muling among younger cohorts.

Recommendation 6

An adaptable approach should be adopted to tackle low-level money laundering:

a. Depending on the severity of the offence, law enforcement should be granted discretion to either issue a formal warning (Cease and Desist Notice) to first-time offenders, refer culprits to mandatory re-education programme, or pursue prosecution if appropriate.

b. Where offending continues, law enforcement should have the option to impose a civil penalty, such as a fixed penalty notice.

c. Where offending further continues or is substantial in the first instance, law enforcement should consider prosecution under the new proposed summary-only money laundering offence, the Proceeds of Crime Act 2002 or other relevant legislation.

d. Guidance should be issued, by the National Police Chiefs' Council and Crown Prosecution Service, to help law enforcement identify vulnerable individuals, including those who may have been coerced into offending.

Recommendation 7

Create a summary-only offence for low-level money laundering—allowing a bank account to be used directly or indirectly by another person without a reasonable excuse.

[290] See chapter 'Education and Awareness'.

8. Detection and Disruption

353. Having examined the enabling architecture of fraud, including identity theft, digital impersonation, deed poll abuse, and money muling, I now turn to the first operational step in the State's response: detection. If fraud is to be tackled effectively, it must first be identified. Without robust detection mechanisms, fraudulent activity remains hidden, undermining both prevention and enforcement efforts. This chapter considers the current fraud detection and disruption methods, highlighting the challenges in identifying incidents and the strategic shift towards upstream intervention.

354. As I have noted in the chapter 'Contemporary Picture', there is a disparity between the figures estimated by the Crime Statistics for England and Wales (CSEW), 4.1 million fraud offences, and those reported to Action Fraud (299,046).[291]

355. The divergence arises from methodological differences. Action Fraud[292] relies on voluntary reporting, subject to biases and barriers. CSEW, by contrast, uses household surveys and extrapolation, capturing incidents regardless of police or Action Fraud involvement. The result is that the CSEW figures, while they rely on extrapolation, are more representative, whilst Action Fraud data is constrained by public awareness and trust. This is indicative of a deeper mistrust and disillusionment which is deterring individuals and companies from reporting fraudulent activity.

<u>Barriers to Reporting</u>

356. Evidence gathered by this Review identifies four principal barriers to reporting:

   a. Difficulty navigating and understanding the reporting systems.

   b. Little faith in law enforcement.

   c. A sense of shame among victims.

   d. Corporate fear of reputational damage.

357. These factors are compounded by the nature of fraud itself. Unlike physical crimes, fraud is rooted in deception and often perpetrated anonymously. Victims may not realise they have been defrauded until long after the event. Even then, they may be unable to identify the perpetrator or may feel emotionally compromised, reducing their desire to submit a formal report.

---

291 Office for National Statistics, *Statistics on Crime in England and Wales* (2025), appendix table Year to March 2025.
292 Replaced by the Report Fraud service on 4 December 2025.

Action Fraud and the Intelligence Gap

358. A key issue historically plaguing detection of 'volume' fraud incidents is lack of understanding of the reporting services. In 2019, HM Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) noted that "lack of public awareness of Action Fraud" was a key reason why fraud was not reported.[293] Responding to this, the previous government developed a national anti-fraud campaign known as 'Stop! Think Fraud', in February 2024.[294] The campaign was successful in not only raising awareness of Action Fraud, as the national reporting service, but also in preventing potential frauds by providing individuals with clear guidance on how they can protect themselves.

359. But for those individuals who have managed to locate the service, their confidence in law enforcement's ability to tackle the fraud is undermined by the dismal reality of the investigative outcomes. Of the 299,000 cases reported to Action Fraud in the year ending March 2025, 42,847 cases were disseminated to local police forces for investigation in the same year.[295] Of those investigated, 80% resulted in no further action.[296]

360. Given this record, Action Fraud has suffered from a poor public reputation. In 2019, *The Sunday Times* investigated the service and found that victims of fraud were misled by call handlers into thinking that their cases would be investigated, whilst the majority were not disseminated to investigative forces.[297]

361. Following this report, City of London Police raised matters with Sir Craig Mackey, the then Deputy Commissioner of Action Fraud. His review noted that both Action Fraud and the National Fraud Investigation Bureau (NFIB) had the potential to serve policing, but that their operations were "significantly hampered by an operating system that is not fully functional and resourcing levels that have not kept pace with increased reporting".[298]

362. In 2021, the Government published a response to his initial report. The report stressed that, whilst Action Fraud had supported forces in identifying and communicating with vulnerable fraud victims, the performance of the call service remained poor. "The average call waiting time and abandonment rate remain too high," the report noted. The report also asserted that the NFIB's intelligence database, Known Fraud, "was not fit for purpose", and it called for a new intelligence system.[299]

---

[293] HM Inspectorate of Constabulary and Fire & Rescue Services, *Fraud: Time to Choose, An inspection of the police response to fraud*, (2019), [Accessed 17 September 2025].
[294] Gov.uk, 'Major campaign to fight fraud launched', news story, 12 February 2024, [Accessed 17 September 2025].
[295] Office for National Statistics, *Statistics on Crime in England and Wales* (2025).
[296] Home Office, *Crime outcomes in England and Wales: 2024-2025*, year to March 2025, table 5.3.
[297], Morgan-Bentley, P. and Good, A., *Action Fraud investigation: victims misled and mocked as police fail to investigate*, video, 14 August 2019, *The Sunday Times*, [Accessed 17 September 2025]
[298] HM Inspectorate of Constabulary and Fire & Rescue, *Fraud: Time to Choose, An inspection of the police response to fraud*, (2019), [Accessed 17 September 2025].
[299] Ibid.

363. It is worth noting that much of the criticism of Action Fraud is that the service does not investigate fraud. However, that was never the purpose behind this agency—it was intended to provide a reporting and analysis 'front door' before disseminating to the relevant investigative agency. Consequently, Action Fraud continues to bear the blame, in part, for decisions by local police forces not to progress disseminated cases.

Fraud and Cyber Crime Reporting and Analytics Service: A New Approach

364. In its 2023 Fraud Strategy, the Government acknowledged longstanding concerns regarding the effectiveness of existing mechanisms for reporting fraud.[300] As part of its stated commitment to reform, the Government announced its aim to replace Action Fraud with a new service: the Fraud and Cyber Crime Reporting and Analytics Service (FCCRAS), now referred to as 'Report Fraud'. This new service has replaced the functions previously performed by both Action Fraud and NFIB.[301]

365. Report Fraud is designed to enhance accessibility for victims of fraud.[302] The services include a redesigned website intended to be more user-friendly, and an expanded call centre. The Government is estimating that the new service will have double the capacity, with an anticipated capability of managing in excess of one million calls per annum. Whether this projection will be realised in practice remains to be seen.

366. The City of London Police also intend to incorporate a triage function to identify cases that are not suitable for further investigation. In such instances, victims are to be referred to the Report Fraud Victim Services (formally the National Economic Crime Victim Care Unit (NECVCU)), which is now established across all 43 police forces in England and Wales. The purpose of this is to reduce the risk of repeat victimisation and to provide consistent support for those more vulnerable victims with onward referrals to other agencies as appropriate. Police forces are now able to access victim data within their jurisdictions.

367. The new Report Fraud analytics function, FCCRAS, operates on a cloud-based platform and utilises automation and artificial intelligence (AI) to enhance its functionality. It is anticipated that these technologies will significantly increase the volume of intelligence packages generated, potentially up to 80,000 annually, compared with the current average of 24,900.[303] A prioritisation framework, based on vulnerability, harm and solvability, is being used to support faster crime dissemination, safeguarding referrals and improved victim updates. The Review has also been informed of a strategic pivot towards

[300] Home Office, *Fraud Strategy: stopping scams and protecting the public*, (2023), CP 839.
[301] Home Office, *Next Generation Fraud and Cyber Crime Reporting and Analysis Service (FCCRAS) Project Accounting Officer Assessment,* (2022), [Accessed 17 September 2025].
[302] Ibid.
[303] Estimated data provided by the Home Office.

industrialised disruption, underpinned by enhanced data-sharing across Government, law enforcement, and industry.

368. While the proposed reforms are welcome, the service must operate transparently and be accountable to clear performance standards. The Review recommends that Report Fraud publicly commit to a defined timeframe, such as a 14-day target, for updating victims on the progress of their reports. Above all, the new service must not lose sight of its primary purpose: to serve victims. Their experience must remain central.

Recommendation 8

Report Fraud should publicly commit to a 14-day service standard, ensuring that every victim receives a clear update on the status of their report within that timeframe. This commitment should cover three key elements:

a. Acknowledgement and Case Reference – Immediate confirmation of the report with a unique reference number.

b. Triage Decision – Completion of an initial assessment and prioritisation within 14 days, with the outcome communicated to the victim.

c. Accessible Progress Tracking – Provision of a secure, user-friendly platform enabling victims to monitor progress, view updates and access support resources at any time.

369. Replacing the existing service with Report Fraud will undoubtedly go some way toward restoring public trust. However, it must be recognised that fraud, by its very nature, presents enduring barriers to reporting. It is a crime rooted in deception, often perpetrated anonymously and discovered only after the fact.

370. Victims may feel shame, confusion, or betrayal, particularly in emotionally manipulative offences such as romance fraud, while businesses may fear reputational damage. These dynamics, both personal and institutional, contribute to persistent under-reporting. Even with improved infrastructure, the hidden and psychologically impactful nature of fraud will continue to inhibit disclosure. The system must therefore be designed not only to receive reports but to actively encourage them, recognising the unique challenges posed by this type of offending.[304]

Duty to Report Fraud

371. Given the significant under-reporting of fraud, this Review heard proposals regarding mandating reporting for private individuals and companies outside the regulated sector.

[304] See chapter 'Victims'.

Currently, 87% of fraudulent activity goes unreported, leaving a substantial intelligence gap and limiting law enforcement effectiveness. Such a system could dramatically improve the intelligence picture and enable more proactive enforcement, while also offering victims a clearer path to redress.

372. However, mandatory reporting raises practical and ethical challenges. Imposing penalties for non-compliance would effectively punish victims twice, first through the fraud itself, and then through legal sanctions for failure to make a report. Internationally, while some jurisdictions have enacted failure-to-report statutes for serious crimes, most stop short of requiring fraud to be reported. This reflects a recognition that mandatory reporting in fraud cases could ultimately harm victims rather than protect them.

373. With this said, corporations and regulated sectors fall into a different category from individuals, and there are sensible expectations that companies will not only report fraud but actively support efforts to detect and disrupt illicit activity. This has already been explored in an earlier chapter, 'Corporate Responsibility'. Also, for individuals and companies operating in the regulated sector, their obligation to make a suspicious activity report where another person has been engaged in fraudulent activity should not be overlooked in this context.[305]

Disruption

374. Detection and disruption are not sequential stages but interdependent functions. The efficacy of one determines the success of the other. Effective disruption depends first and foremost on early and accurate detection. The sooner fraudulent activity is identified, ideally in real time, the greater the opportunity for law enforcement and partners to intervene before harm is done. Early detection enables a pivot from reactive investigation to proactive disruption, and in some cases even pre-emptive action that prevents fraud from reaching victims altogether. Conversely, proactive disruption can illuminate patterns that enhance future detection, reinforcing a cycle of intelligence-led enforcement.

375. The 2023 Fraud Strategy reflects this shift in emphasis. It committed to a closer working between law enforcement and United Kingdom (UK) intelligence agencies, to share intelligence in real time to disrupt criminal fraudulent operations before they cause harm.[306] This whole-system approach is designed to make the UK a more hostile environment for fraudsters, both domestic and international.

376. A central component of the Government's first fraud strategy was the creation of the National Fraud Squad (NFS), jointly led by the National Crime Agency (NCA), the National Economic Crime Centre (NECC), and the City of London Police (CoLP).

305 Section 330(1) of the Proceeds of Crime Act 2002.
306 Home Office, *Fraud Strategy: stopping scams and protecting the public*, (2023), CP 839.

Comprising approximately 500 specialist posts,[307] the NFS represented both the recruitment of new fraud investigators and the formal identification and designation of existing fraud specialists within law enforcement. Officers are not co-located but operate as a distributed network across national, regional and local policing units, unified by a single strategic mandate: to drive proactive, intelligence-led enforcement against serious fraud. This rebadging exercise ensures that fraud expertise is recognised and mobilised across the policing ecosystem, regardless of geographic location. The network is also designed to increase intelligence flows and enable coordinated disruption of fraud networks operating both domestically and overseas.

377. The Fraud Targeting Cell (FTC), a multi-agency unit staffed by the NCA and CoLP with wider attachments, builds proactive, suspect-led intelligence on the highest-harm UK fraud offenders and feeds packages to the NFS for regional, national and international action.[308]

378. In parallel, the Government is establishing the Online Crime Centre (OCC) This Review was told that the initiative will facilitate intelligence sharing between law enforcement and the private sector, enabling the identification, blocking and disruption of online criminality. The desire is that the OCC will also support efforts to identify victims in need of assistance.

379. To tackle business-enabled fraud, there is the Single Network Analytics Platform (SNAP), first launched in 2023, a cross-government cloud system aimed at proactively detecting and preventing fraud and economic crime in the public and UK's financial services. The system has recently been updated to SNAP 2.0, which will enable the Financial Conduct Authority and Companies House to identify shell companies and bad actors.[309]

380. This Review supports this strategic pivot towards disruption, recognising the significant jurisdictional and evidential challenges in prosecuting fraudsters, many of whom operate from overseas. While accountability remains essential, the scale and complexity of modern fraud demand a proactive posture. The State cannot afford to wait for victims to report offences; it must instead use real-time intelligence to undermine the business models of serious organised crime groups and render them unworkable.

381. In operational terms, law enforcement is already devoting additional attention to disruption: the NCA reports a record 6,989 disruptions in 2024 and has stopped more than 400,000 fraud attempts, preventing an estimated £221 million in harm.[310] CoLP likewise records high volumes of technical and organised crime gang-linked interventions, 239 fraudulent websites and 12,522 payment accounts were disrupted in the third quarter

[307] Ibid.
[308] National Crime Agency, *Annual Report & Accounts 2024–25*, (2025), page 5.
[309] Horton, C., 'UK government upgrades its fraud detection capabilities', THINK Digital Partners, 21 March 2024.
[310] National Crime Agency, *Annual Report & Accounts 2024–25*, (2025).

of 2024[311], while the National Cyber Security Centre continues to actively take down businesses fraudulently posing as Government departments or bodies.[312]

382. This approach also has downstream benefits. By reducing the volume of successful fraud attempts, the burden on local police is eased, freeing up capacity to investigate the cases that do reach them. However, the success of these efforts must ultimately be judged not only by operational metrics but by the experience of victims. Disruption is not an end in itself. It must serve the broader goal of protecting the public, and in doing so, ensure that victims remain at the heart of the system.

Conclusion

383. The current system for reporting fraud is fragmented and underutilised, leaving law enforcement with significant gaps in its intelligence picture. The introduction of the Report Fraud service represents a substantial investment in infrastructure and capability. Its design, combining improved accessibility, triage and enhanced analytical tools, has the potential to address long-standing deficiencies in victim engagement and data collection.

384. Whether these ambitions will be realised remains uncertain. The effectiveness of the new model will depend on sustained operational delivery, clear performance standards, and public confidence in the reporting process. If successful, the service could transform the State's ability to understand the true scale of fraud, replacing the current opacity with a coherent and comprehensive dataset. Such visibility is not a peripheral improvement; it is fundamental to an intelligence-led response. Without it, enforcement agencies will continue to operate with significant blind spots that compromise strategy and deterrence. With it, the foundations for a more proactive and integrated approach to fraud prevention and disruption can be properly established.

[311] City of London Police, *Performance Report Q3 2024/25*, (2025).
[312] House of Lords Written Answer, *NCSC Takedown Service*, (2025), HL4186.

9. Public–Private Partnerships

385. It would be unrealistic to suppose that the State could, unaided, overcome the escalating threat of fraud without meaningful collaboration from the private sector, a view expressed by Lord Goldsmith, then Attorney General in 2006, and one that remains no less compelling today.[313] The scale of modern fraud, spanning multiple platforms and sectors, demands frameworks that enable public authorities and private actors to work together, and at speed. There are obvious advantages for the private sector as firms wish to avoid either themselves, or their clients, falling victim, and do not want to be used as conduits for fraudulent activity, which can dent the value or reputation of a business.

386. Correctly structured public–private partnerships (PPPs) are an essential component of an effective modern fraud response, though they are no panacea. They must, however, be designed with care: established in law, transparent in purpose, and subject to robust accountability. The State should not be content to let such partnerships stand on unsteady foundations which will be unlikely to stand the test of time.

387. For present purposes, I use PPPs to describe formal or informal frameworks through which the Government, law enforcement and regulators work with businesses to share intelligence, set joint priorities and/or deliver operational outcomes in the public interest. That may range from compelled information flows (e.g. statutory reporting duties) to voluntary, cooperative taskforces with two-way sharing and jointly agreed objectives, or to contractual relationships between a public authority and a business to investigate and/or commence civil or criminal proceedings.

Development of Public–Private Partnerships

388. Post-war Britain relied heavily on nationalised undertakings to provide core services, such as transportation and telecommunication. The traditional model during this period was for the State to build or purchase the physical assets and to use either public sector employees or private contractors to maintain its operations. However, this model ultimately proved too inefficient and costly and suffered from issues of corruption and overstaffing. They were deemed no longer viable and thus began a transition to utilising the private sector.[314]

389. From the 1980s onwards, successive administrations turned to private capital and capability to finance and operate public projects. Early UK examples commonly cited in the PPP literature include the Dartford–Thurrock Crossing (concession financing for the

---

313 Attorney General's Office, *Fraud Review,* (2006), page 7.
314 Doloi, H.K. and Ma, Z., '[Balancing value-for-money and operational performance of public–private partnerships projects]', conference paper, 14 July 2010.

Queen Elizabeth II Bridge)[315] and the Severn Bridge concessions;[316] the modern Private Finance Initiative (PFI) was formally adopted in 1992.[317]

390. In the economic crime sphere, the UK has had a public private partnership capability for more than ten years. The National Economic Crime Centre (NECC) was established within the National Crime Agency (NCA) in 2018 precisely to 'corral' public and private capabilities against economic crime.[318] The NECC houses the Joint Money Laundering Intelligence Taskforce (JMLIT), a mature PPP of more than 200 organisations spanning law enforcement, regulators, major financial institutions, telecoms, technology, professional services and more.[319]

391. The 2023 Economic Crime Plan 2 made PPP the central method of delivery, across money laundering, kleptocracy and fraud, and commits both sectors to a shared programme of work.[320] In parallel, the 2023 Fraud Strategy[321] coupled new law-enforcement capacity with expectations of industry action, particularly from technology platforms whose services are increasingly exploited for fraud. The 2023 Online Fraud Charter[322] then set voluntary, time-bound commitments for major technology firms to block and remove frauds, engage with law enforcement, and share intelligence ahead of full regulatory implementation under the Online Safety Act 2023.

392. The United Kingdom's (UK) approach is similar to that of its international partners. The Financial Crimes Enforcement Network (FinCEN) Exchange in the United States, launched in 2017 and given an express statutory basis by §6103 of the Anti-Money Laundering Act 2020[323], provides a useful comparator for placing PPPs on a firm legal footing while protecting appropriate information flows.[324] Australia's Fintel Alliance (AUSTRAC) likewise illustrates how real-time data collaboration across Government, banks and other sectors generates tangible disruption outcomes.[325]

---

315 The Dartford–Thurrock Crossing Tolls Order 1990.

316 Severn Bridge Act 1992.

317 Richards, M., Calder, K. and Handril, A., 'United Kingdom', in Freire, A.L, et al.(Eds.), *The Public–Private Partnership Law Review*, sixth edition, London: Law Businesss Research, (2020), pp. 252-256.

318 National Crime Agency, 'National Economic Crime Centre', [Accessed 23 September 2025].

319 Ibid.

320 HM Treasury and Home Office, *Economic Crime Plan 2 – 2023-2026,* (2023).

321 Home Office, *Fraud Strategy: stopping scams and protecting the public*, (2023), CP 839.

322 Home Office, *Online Fraud Charter*, (2023).

323 US Code, *Anti-Money Laundering Act §6103*, (2020).

324 Financial Crime Enforcement Network, 'FinCEN Exchange', [Accessed 3 September 2025].

325 AUSTRAC, 'Fintel Alliance', [Accessed 3 September 2025].

Two models of collaboration

Compelled Collaboration

393. A significant part of 'partnership' is in fact compulsion by law. The regulated sector is under criminally enforceable duties to make disclosures of suspicions of money laundering (the s.330 Proceeds of Crime Act 2002 (POCA) 'failure to disclose' offence), with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017[326] (MLRs) providing the compliance architecture. There are analogous provisions under counter-terrorist financing legislation. Key components of this framework include the mandating of risk assessments, record keeping, customer due diligence checks, the employment of Money Laundering Reporting Officers (MLROs), training and internal controls.[327] These are core, one-way channels: the private sector must report to the State.

394. The legislative framework is further supported by the Economic Crime and Corporate Transparency Act 2023 (ECCTA), which introduced a strict liability for large companies that fail to have reasonable fraud prevention procedures in place. It also provides safe harbours that give firms further confidence that preventative sharing will not attract civil liability when done correctly.

395. While the legislative framework imposes enforceable duties on the regulated sector, it remains fundamentally reactive. Statutory obligations compel firms to report suspicions and maintain compliance controls. However, these mechanisms are largely one-directional. They mandate minimum standards of reporting but do not foster mutual engagement or strategic collaboration.

396. Much of the existing legislation around data-sharing provides legal gateways through which firms may disclose information without breaching privacy laws or attracting regulatory sanction. These gateways, while operationally useful, do not constitute a framework for structured, intelligence-led collaboration. The responsibilities of relevant regulators and the limitations of current data-sharing models are considered further in the next chapter.

Voluntary Collaboration

397. At the other end of the spectrum lie voluntary PPPs: structures where both sides see incentive and value in strategic and operational cooperation. These partnerships come in a variety of forms, but for the sake of brevity I will focus on three broad categories: strategic, operational and enforcement.

[326] The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.
[327] Law Society, *Quick guide to the Money Laundering Regulations 2017*, (2020).

398. **Strategic partnerships** foster collaboration between public and private sectors to shape the direction of policy, align priorities, and build consensus around a shared operational framework. These structures are not merely consultative; they serve as platforms for coordinated planning, horizon scanning, and the development of sector-wide responses to emerging threats.

399. The standout example is the Joint Fraud Taskforce (JFT)[328]—a Home Office-convened strategic partnership, launched in 2016, which convenes private sector, law enforcement and Government departments, to collectively tackle fraud.

400. JFT's achievements include the creation of Fraud Sector Charters.[329] The taskforce has been successful in securing sector-specific voluntary agreements with major companies in insurance, technology, accountancy, retail and telecommunications. These voluntary charters establish common strategic goals in the fight against fraud.

401. **Operational partnerships** aim to support both law enforcement and the private sector in the delivery of their operations. In the case of fraud, this can range from data-sharing between different sectors to proactively disrupting fraud and promoting fraud awareness.

402. One such example is the Joint Money Laundering Intelligence Taskforce, established in 2015 as a Home Office–NCA pilot and then mainstreamed, which facilitates real-time tactical intelligence sharing for the purposes of tackling money laundering. As previously mentioned, JMLIT has been successful in aiding officers to identify unknown accounts, building the evidence base to arrest suspects; and in restraining suspected criminal funds.[330]

Case Study – The Joint Money Laundering Intelligence Taskforce (JMLIT)[331]

Launched in 2015 as a 12-month pilot, JMLIT has become a permanent feature of the UK's response to financial crime. It provides a secure forum for two-way information sharing between law enforcement and the financial sector, operating through:

a. An Operations Group for case-specific intelligence exchanges.

b. Threat Groups and short-term 'cells' focused on emerging risks such as fraud, high-end money laundering and crypto-crime.

[328] Home Office, 'Joint Fraud Taskforce', (2017), [Accessed 3 September 2025].
[329] Ibid. See also chapter 'Short History of Fraud' in this Review.
[330] National Crime Agency, 'National Economic Crime Centre', [Accessed 23 September 2025].
[331] Ibid.

By December 2024, JMLIT "plus" had identified over 10,700 previously unknown accounts, closed 8,100 accounts, supported 391 arrests, and helped restrain £248 million in suspected criminal funds, alongside issuing 100 national alerts.

403. The Dedicated Card and Payment Crime Unit (DCPCU) is another operational partnership. This is a specialist national police unit funded by the banking industry through UK Finance and staffed by the City of London Police (CoLP) and the Metropolitan Police Service.

404. Its mandate is specifically to "investigate, target and, where appropriate, arrest and seek successful prosecution of offenders responsible for fraud affecting the payments, banking and finance industry". It works alongside the private sector towards this goal and has a Protect team which is responsible for delivering education and awareness products to the members and the public to reduce financial fraud. DCPCU has been credited with preventing or disrupting fraud leading to c. £750 million in industry savings since its inception.[332]

405. **Enforcement partnerships** are joint initiatives in which public bodies are outsourcing a particularly resource-intensive aspect of their work to the private sector to undertake.

406. The partnership between international law firm Gowling WLG and CoLP represents a novel enforcement model in the fraud recovery landscape.[333] Under this arrangement, Gowling's Civil Fraud and Asset Recovery team works alongside law enforcement to pursue civil recovery of assets in cases where criminal prosecution is not viable—particularly those involving complex or anonymous digital frauds.

407. This collaboration follows a successful pilot in which the team recovered over £2 million for an elderly woman suffering from Alzheimer's, who had been defrauded through a cryptocurrency scam.[334] The initiative reflects a growing recognition that civil enforcement, when strategically aligned with policing, can offer victims a meaningful route to restitution and bolster the State's broader disruption efforts against organised fraud. The Gowling WLG and CoLP partnership is just one example of a private firm closely collaborating with an enforcement authority to carry out work that has traditionally been the responsibility of the State. I am aware that there are other such partnerships.

408. These initiatives illustrate the breadth of voluntary PPPs, from strategic priority-setting to greater data-sharing, to active support on live operations.

---

[332] UK Finance, 'Dedicated Card and Payment Crime Unit', [Accessed 17 November 2025].
[333] City of London Police, 'City of London Police partner with international law firm Gowling WLG to help victims of fraud recover their money', press release, 3 April 2025.
[334] Ibid.

Mutual Benefit

409. Having outlined the forms that these partnerships can take, it is worth considering the relative benefits of such initiatives for both the State and the private sector. I examine these perspectives in turn.

<u>Benefits for the State</u>

410. **Tackling fraud upstream and live disruption** – One of the key benefits of this initiative is that it shifts policing efforts from responding to reports to proactively working with industry to confront the threat from first-line visibility.

411. For example, the Online Fraud Charter works with technology companies to take down online fraudulent pages upon detection, thereby preventing victims from falling prey to potential scams. Similarly, data-sharing enabled through JMLIT allows for live data-sharing with financial services and law enforcement to actively prevent money-laundering when detected.

412. **Strengthens cross-industry intelligence** – Collaboration between the public and private sectors provides an effective means of improving intelligence gathering as it enables for effective monitoring across multiple industries.[335]

413. Currently, the National Fraud Intelligence Bureau (NFIB), receives reports from a range of sources, including industry reporting, which helps to inform the police's threat assessment of fraud and how resources should be allocated. As previously discussed, the Government is looking to launch an Online Crime Centre (OCC), which will facilitate greater intelligence sharing between law enforcement and the private sector. This will support the identification, blocking and disruption of online criminality as well as victim support services.

414. **Leverage private analytic capacity, technology and resources –** Given the resource limitations of public services, PPPs offer a means in which they can leverage private firms to make use of their analytical capacity, technology and resources. This may be evidenced by the Gowling WLG–CoLP partnership, which will aid victims of fraud to recover their finances where a criminal procedure is not possible. In this case, the programme depends on the capacity of a private firm to aid law enforcement. In a similar vein, DCPCU leverages data analytics, intelligence and technology from the private sector in support of its goals of disrupting criminal activity and recovering assets.

415. **Builds consensus** – In contrast to compelled cooperation, voluntary PPPs can foster a greater sense of collaboration and compliance across industry. JFT provides the

[335] This is discussed in greater detail in the chapter 'Detection and Disruption'.

Government with an opportunity to communicate its strategic priorities to industry and reduce its blind spot by hearing about the evolving fraud threat impacting the private sector. The various fraud charters are a testament to the positive work that can be achieved through this initiative.

Benefits for the Private Sector

416. PPPs offer tangible operational and strategic benefits to the private sector. Chief among these is access to public-sector intelligence, which can materially enhance firms' ability to conduct robust customer due diligence checks required under the MLRs, as well as assess whether they are at risk of money laundering and take proportionate preventative measures. The ability to share and receive information about customer risk profiles strengthens internal safeguards, reduces exposure to fraud, and improves protections for clients.

417. These partnerships also accelerate investigative feedback loops. Structured engagement with law enforcement enables firms to receive timely intelligence on emerging threats, refine their risk assessments, and adapt compliance protocols accordingly. The Financial Crimes Enforcement Network (FinCEN) Exchange in the United States is instructive: by convening financial institutions, law enforcement and national security agencies, it has improved the quality and utility of suspicious activity reports and fostered more responsive threat identification.[336]

418. The effectiveness of this model was demonstrated following Russia's invasion of Ukraine.[337] In response, FinCEN issued five alerts concerning sanctions evasion and other illicit financial activity linked to individuals associated with the Russian regime. These alerts prompted a surge in reporting from financial institutions, which directly informed FinCEN's analysis and supported both law enforcement and the wider financial sector.

419. Participation in PPPs also confers reputational benefits. Firms that collaborate with law enforcement demonstrate a visible commitment to financial integrity and public protection. This proactive stance reinforces trust among consumers, investors and regulators, and positions firms as responsible actors in the fight against economic crime.

420. Finally, PPPs offer the private sector a seat at the table in shaping policy and regulatory priorities. Engagement with the Government enables firms to understand the strategic direction of fraud enforcement, influence the development of regulatory frameworks, and align their compliance resources with national priorities. The Second Economic Crime

336 Financial Crimes Enforcement Network, 'FinCEN Exchange', [Accessed 17 September 2025].
337 U.S. Department of the Treasury, *2024 National Strategy for Combating Terrorist and Other Illicit Financing*, (2024), page 19.

Plan[338] explicitly commits to working with industry to define the threat landscape and set enforcement priorities, an approach that supports more efficient and targeted compliance.

Risks and Hazards

421. No partnership framework is without risk. The concerns outlined below are far from theoretical; they are rooted in recent UK experience and must be taken seriously if the Government is to continue leveraging PPPs, including its proposed new OCC.

422. **Misaligned incentives** – In approaching PPPs, we must recognise the significant different vantage points of both the public and private sectors. The private sector's participation in PPPs is typically guided by commercial imperatives, not altruism. Firms engage where collaboration aligns with shareholder interests, operational efficiency or reputational gain.

423. Beyond financial concerns, we can recognise potentially significant differences in risk appetites, the willingness to allocate resources, and whether the speed of delivery or due diligence is prioritised. The private sector may favour speed and risk-taking to deliver shareholder value, while the public sector, mindful of reputational and political consequences, may prioritise caution and due process. Similarly, firms may resist resource-heavy initiatives that dilute return on investment, whereas the State may fund such efforts in pursuit of public interest. The characterisation provided is extremely broadbrush, but it serves to remind policymakers of the divergent incentives the public and private sector will hold.

424. **Equality before the law** – Private entities are organised to conduct business, not to dispense justice. When investigatory or prosecutorial boundaries are blurred, whether through formal delegation or informal assumption, there is a real risk of unfairness, confirmation bias, and defensive decision-making.

425. **Competition and market distortion** – Participation in PPPs can bring reputational benefits and privileged access to intelligence. Opaque entry criteria risk entrenching dominant incumbents and excluding smaller firms or fintech innovators, undermining competition and innovation.

426. To maintain fairness, criteria for participation should be objective, proportionate and published. Where numbers must be limited for security reasons, rotating membership or sectoral representation is preferable to permanent seats. International best practice, including the Organisation for Economic Co-operation and Development (OECD)

338 Home Office and HM Treasury *Economic Crime Plan 2*, (2023).

principles on PPP governance,[339] stresses transparency and value for money, principles that apply as much to financial–crime partnerships as to infrastructure projects.

427. **Accountability and transparency** – When responsibilities are divided between public authorities and private firms, accountability can become blurred. The Serco/G4S electronic tagging scandal, where systemic overcharging triggered major repayments and penalties[340], illustrates the consequences of weak oversight and misaligned incentives.

428. Since private partners are not subject to the Freedom of Information Act, transparency must be built into the contractual framework from the outset.

429. **Private–public data-sharing** – As discussed in the following chapter, firms are often hesitant to share data with the State, citing privacy concerns and regulatory risk. However, as the Information Commissioner's Office has made clear, "data protection is not an excuse" to avoid sharing information that could prevent fraud.[341]

430. UK law permits data-sharing for law enforcement purposes within strict limits. The Data Protection Act 2018 (Part 3) and the Digital Economy Act 2017 (Part 5) provide lawful gateways. But these frameworks do not permit indiscriminate pooling. To remain lawful and legitimate, PPPs must apply:

   a. Clear role allocation (controller vs processor).

   b. Purpose limitation and necessity tests.

   c. Data Protection Impact Assessments (DPIAs).

   d. Minimisation and retention controls.

   e. Audit trails and secondary use restrictions.

431. Without these disciplines, partnerships risk becoming both legally vulnerable and socially unacceptable.

432. **Public–private data-sharing** – When the State shares sensitive data with private partners, it assumes risk. Mishandling may result in breach or misuse. A subtler risk arises if the partner is later acquired by a hostile actor. The National Security and Investment Act 2021[342] addresses this by requiring screening of acquisitions in sensitive sectors. The

---

339 Organisation for Economic Co-operation and Development, *Recommendation of the Council on Principles for Public Governance of Public-Private Partnership*, (2012).

340 BBC News, 'Serco fined £19m over tagging scandal', 3 July 2019. Serco agreed to pay £19.2 million under a Deferred Prosecution Agreement with the Serious Fraud Office for fraud and false accounting linked to its electronic tagging contract.

341 Information Commissioner's Office, 'Data protection is not an excuse when tackling scams and fraud', news release, 22 November 2024.

342 National Security and Investment Act 2021.

National Cyber Security Centre likewise warns that vulnerabilities can be introduced or exploited at any point in a supply chain.[343] To mitigate risk, PPP agreements should:

a. Include rules that let the Government step in or stop sharing data if the company changes ownership—especially if it is bought by someone with a medium- or high-risk profile.

b. Keep sensitive data separate and anonymised where possible: limit access to only those who truly need it and make sure the Government holds the encryption keys whenever it can.

c. Store important data in the UK or in countries that are trusted and have strong security standards.

d. Check suppliers regularly, not just once at the start, to make sure they stay secure and compliant over time.

433. **Public confidence** – Trust is fragile where justice functions appear privatised. PPPs must be presented, and operated, as mechanisms to strengthen public protection, not bypass due process. Transparency helps: commitments, performance indicators and privacy notices should be published in plain language. Where arrangements are opaque, victims are less likely to engage, undermining the partnership's purpose.

Limits of Private–Public Partnerships in Criminal and Civil Justice

434. PPPs are designed to support State functions. Investigation, charging and prosecution involve coercive powers which require independent oversight. Appropriately conceived, PPPs support intelligence, prevention, disruption and victim protection, and the bringing of court proceedings in appropriate cases. They supplement, but must never substitute, the role of the State in responding to fraud.

Safeguards and Standards

435. To capture benefits while managing risk, I propose the following guardrails for any PPP focused on disrupting or tackling fraud.

436. **Clear statutory gateways and safe harbours** – Build on ECCTA to give participants certainty as to lawful bases, liability protections and conditions for both direct and indirect sharing (request- and warning-conditions). I return to the subject of data-sharing in the next chapter.

[343] National Cyber Security Centre, *Supply chain security guidance*, (2018), [Accessed 31 October 2025].

437. **Purpose-built governance** – Each PPP should have a published charter (purpose, scope, data types, retention schedules), a senior accountable owner in the public sector, and an annual report of activity and impact (subject to necessary operational sensitivities). The Online Fraud Charter format is a useful template for transparent commitments.

438. **Independent oversight** – An oversight panel (with independent members) should review compliance with data protection and competition principles, and audit a sample of operational uses annually. For public-sector sharing, align with the Digital Economy Act 2017 Part 5 codes and registers[344]; for law-enforcement processing, ensure that Data Protection Act 2018 Part 3 documentation (appropriate policy documents, DPIAs) is in place.[345]

439. **Due process protections** – PPP outcomes that affect individuals (e.g. the closure of a person's bank or social media account, social media content takedowns) have proportionate and clear redress pathways. There must be an ability for such measures to be challenged.

440. **Access and competition** – Admission criteria should be objective and proportionate; small and medium-sized enterprises/fintech participation should be facilitated where feasible to avoid undue concentration of influence.

441. **Key performance indicators** – Agree common outcome indicators (e.g. prevented losses, disruptions, arrests/charges attributable to PPP intelligence, victim restitution) and publish them periodically, as JMLIT has done.

<u>Intelligence Sharing and the Case for Statutory Reform</u>

442. Law enforcement alone cannot turn the tide on fraud. A coordinated, intelligence-led response is essential, one that draws on the strengths of both public and private actors. Over the past decade, partnerships such as JMLIT have become central to the UK's economic crime strategy.

443. However, in light of substantial concerns set out in this chapter, the Review recommends placing intelligence sharing within economic crime and fraud-focused PPPs on a statutory footing. This is not a move toward centralisation. It is a legislative imperative: Parliament must define the boundaries of lawful collaboration—clarifying purpose, participation, governance and oversight.

[344] Cabinet Office, *Digital Economy Act 2017 part 5: Codes of Practice*, (2018).
[345] Ministry of Defence, *Law enforcement processing: part 3 appropriate policy document*, (2024).

444. Nor is this a blanket dismissal of PPPs. It is a proposal to formalise a system the UK already relies upon, ensuring it is transparent, accountable, and built to endure. Without strong foundations, even the most effective partnership risks becoming a house of cards.

445. In short, if PPPs are to remain effective, their legal foundation must reflect their strategic importance. The architecture must be deliberate, not improvised, capable of withstanding scrutiny and sustaining impact.

> **Recommendation 9**
>
> Intelligence sharing within public–private partnerships focused on tackling economic crime should take place within a statutory framework.

446. More narrowly, in deciding to partner with private firms to commence legal proceedings which relate to an underlying fraud, law enforcement agencies must remain alert to risks around market distortion, transparency and accountability when engaging private companies. While I wholly support such partnerships where they deliver tangible benefits for victims, they must be subject to fair process. Without open competition and scrutiny, public confidence in these arrangements will erode. I therefore recommend that any collaboration between UK law enforcement and the private legal sector be conducted in a fair, transparent and open manner, with opportunities subject to appropriate oversight and market access.

> **Recommendation 10**
>
> UK law enforcement agencies should collaborate with the private legal sector market in a fair, transparent and open manner, to facilitate the recovery of losses sustained by a victim of fraud.

Conclusion

447. PPPs are not a substitute for the fundamentals of policing, prosecution and judicial determination. But in the absence of structured, lawful and well-governed collaboration with those who own the networks, hold the data and operate the payment rails, the State's response to fraud will continue to lag offenders' methods. The UK Government must prioritise credible fraud-related PPP machinery, including the new OCC.

448. The next step is to ensure these partnerships are transparent, have clear safeguards and are subject to appropriate scrutiny. Executed correctly, PPPs can deliver stronger upstream prevention, faster disruption of criminal activity, enhanced protection for victims, and improved prosecutorial outcomes, while upholding the constitutional principle that justice is a public function, exercised lawfully and in the public interest.

10. Data-Sharing

449. Data-sharing is the lifeblood of effective fraud prevention and criminal investigation. Without it, law enforcement agencies, regulators and private-sector actors operate in silos, each holding fragments of the puzzle, but rarely the full picture. In the context of fraud, this fragmentation allows criminal networks to exploit gaps in oversight, evade detection, and launder illicit gains through increasingly sophisticated means.

450. This chapter explores the current landscape of data-sharing for the purpose of tackling fraud within the criminal justice system, the legal gateways that permit or restrict it, and the operational challenges that hinder its effective use. It draws upon statutory frameworks, case studies and stakeholder insights to argue for a more coherent, proactive and legally confident approach to data-sharing, one that balances privacy with public protection.

Fragmented Ecosystem

451. The UK's approach to fraud prevention is fundamentally constrained by fragmented data sources. Financial institutions, telecoms providers, digital platforms and public authorities each collect valuable data, but there is no centralised visibility into what is held, how it is used, or how it might be shared responsibly.

452. This lack of coordination means that fraud detection efforts are often reactive and incomplete. For example, a single financial institution may only observe 15–25% of its customers' financial activity, making it nearly impossible to detect broader patterns of criminal behaviour without access to external data.[346] This is particularly acute in cases involving money mules—individuals, often vulnerable, who are recruited to launder criminal funds through seemingly legitimate bank accounts. Without cross-sector data-sharing, such operations remain hidden in plain sight.

Current Legal Framework for Data-Sharing

453. In the previous chapter, I outlined how the current legislative framework can be used, in certain circumstances, to compel public and private sector agencies to disclose data which may help inform a criminal investigation. This legislation builds a compliance architecture which mandates a minimum level of data-sharing. It is distinct from legislation aimed at promoting proactive data-sharing by establishing legal gateways. These safe harbours give assurance to public and private bodies that they are able to share data without facing legal sanctions. The legislation thus falls into three categories:

[346] The Payments Association, *Data Sharing to prevent Economic Crime*, (2023), page 8.

a. Mandating the disclosure of information.

b. Requiring self-reporting and sanctions negligence.

c. Providing legal safe harbours for proactive data-sharing.

454. I outline some of the key legislation falling under these categories below.

Compelled Data-Sharing

455. **Criminal Justice Act 1987** – This Act was enacted with the express purpose of addressing serious and complex fraud. It established the Serious Fraud Office (SFO) and conferred upon it unique investigatory powers.

456. Under Section 2, the SFO may compel individuals and corporate entities to produce documents relevant to an investigation into serious or complex fraud, and to attend interviews for questioning. These powers are investigatory in nature and do not require judicial authorisation. Failure to comply with a Section 2 notice constitutes a criminal offence, punishable by fine or imprisonment.

457. **Companies Act 1985** – Section 447 of the Companies Act empowers the Secretary of State to require companies to produce documents for the purpose of investigating their affairs. This power is typically exercised in cases involving suspected misconduct or regulatory breaches. However, Section 449 imposes strict limitations on the disclosure of such information. Disclosure is prohibited unless the recipient is listed in Schedule 15C, or the information falls within the exceptions set out in Schedule 15D.

458. Notably, the National Crime Agency (NCA) is excluded from Schedule 15C, which raises legitimate concerns about investigatory blind spots.

Self-Reporting and Sanctioning Negligence

459. **Proceeds of Crime Act 2002** – Section 330 introduced a criminal offence for the failure to disclose knowledge or suspicion of money laundering. This applies to those working within the regulated sector. Disclosures are typically made via suspicious activity reports (SARs) to the NCA. As noted, this legislation is reliant on individuals within the regulated sector self-reporting as opposed to complying with a direct disclosure order.

460. **Economic Crime and Corporate Transparency Act 2023** – Section 199 establishes strict liability for large companies that fail to prevent fraud by an associated person intending to benefit the organisation or its clients. The only defence is if the organisation had reasonable fraud-prevention procedures in place at the time the fraud occurred.

Legal Safe Harbour

461. **Criminal Justice Act 1987** – Section 3 of this act allows the SFO to share information with Government departments and competent authorities for criminal investigations, including international cooperation.

462. **Crime and Courts Act 2013** – Section 7 allows any person, including another enforcement authority, to disclose information to the NCA for the exercise of its functions, including crime prevention and prosecution. Section 7 also allows the NCA to disclose information in connection with the exercise of any NCA function if the disclosure is for any 'permitted purpose'.

463. **Commissioners for Revenue and Customs Act 2005** – Section 21(a) and (b) Permit HM Revenue and Customs (HMRC) to share information with the Crown Prosecution Service (CPS) for criminal proceedings.

464. **Anti-Terrorism, Crime and Security Act 2001** – Section 19 of the Anti-terrorism, Crime and Security Act 2001 permits HMRC, where proportionate and compliant with data-protection law, to disclose information, including proactively, to support criminal investigations or proceedings in the UK or abroad. This includes disclosure to any prosecutorial or investigative bodies (including intelligence services), whether in the United Kingdom (UK) or internationally, for criminal matters.

465. **Data Protection Act (DPA) 2018** – Schedule 1, Part 2 of the DPA specifically allows for the sharing of data with 'anti-fraud organisations', also known as Specified Anti-Fraud Organisations (SAFOs) for the purpose of preventing fraud.[347] This Act modernises aspects of the Serious Crime Act 2007. SAFOs include Cifas, Experian, and the Insurance Fraud Bureau.

466. **Economic Crime and Corporate Transparency Act (ECCTA) 2023** – Section 188 permits direct information sharing between firms in the regulated sector for the purpose of preventing, detecting, and investigating economic crime. Section 189 allows for indirect sharing of customer information via a third-party intermediary, such as a trusted platform or service provider.

467. This legislation is specifically aimed at providing participants with certainty as to lawful bases, liability protections and conditions for both direct and indirect sharing. Sections 190–193 provide further details on permitted recipients, conditions for lawful sharing, oversight and compliance mechanisms, and interaction with existing data protection laws.

[347] Data Protection Act 2018, Schedule 1, Part 2.

468. **Data (Use and Access) Act 2025** – Sections 2 and 3 allow for firms in the regulated sector to share customer information with one another upon request, given that appropriate safeguards have been followed and there is a genuine economic crime concern.

Voluntary Data-Sharing

469. Alongside this legal framework stand voluntary consortiums, public–private initiatives and non-legally binding memorandums of understanding between public and private sector agencies as well as with foreign governments which facilitate data-sharing.

Case Study – Cifas National Fraud Database[348]

Initially launched in 1988, this consortium currently hosts over 750 members across various public and private sectors and serves two purposes:

1. **Identifying suspicious activity** – Members are able to pool data together and help each other to check if an individual or application has been flagged for fraudulent activity—ensuring the organisation is able to make an informed decision on whether to proceed with a transaction or account.
2. **Supporting victims** – Cifas enables individuals at risk of identity fraud to undertake a protective registration. This registration prompts members to conduct extra checks when these individuals apply for products or services. Such a service can also protect targets through messaging and education.

Case Study – NCA–UK Banks Public–Private Partnerships[349]

Since 2024, the NCA has partnered with seven UK banks to identify and prevent financial criminal networks. Participating banks provide the NCA with account data indicative of potential criminality. Subject matter experts and investigators from the NCA and the banks have formed a joint team to analyse the data, alongside the NCA's own data. Any intelligence outputs will inform the NCA's investigative work and help the banks to identify risk.

The NCA has reported that, since the project went live in 2024, eight new criminal networks have already been identified.[350] Additionally, a further three suspicious networks have been identified and referred to the NCA's intelligence division for further examination, while new leads have been uncovered relating to ten of the agency's largest ongoing investigations.

[348] Cifas, 'National Fraud Database', [Accessed 18 November 2024].
[349] National Crime Agency, 'Ground breaking public private partnership launched to identify criminality using banking data', news release, 26 July 2024.
[350] Gibbon, R. and Fisher, K., *Promising Results from Groundbreaking FinCrime Data Sharing Project Between Seven UK Banks and the National Crime Agency*, blog, 9 January 2025, Squire Patton Boggs.

Regulators

470. Having outlined the legal infrastructure which enables data-sharing, I turn to examine the regulators which oversees data-sharing across different sectors.

471. **Financial Conduct Authority (FCA)**[351] – The FCA regulates UK financial services firms, setting standards, supervising compliance and enforcing accountability. Its objectives are to protect consumers, safeguard the integrity of the financial system, promote effective competition, and, since 2023, support international competitiveness and growth, while requiring authorised firms to maintain controls to prevent financial crime.

472. The FCA ensures compliance with the Financial Services and Markets Act 2000, Electronic Money Regulations 2011, Payment Services Regulations 2017 and most recently, Data (Use and Access) Act 2025. The FCA works with the Payment Systems Regulator (PSR) and Bank of England on data-related aspects of payment infrastructure. It is worth noting that, in September 2022 a new power was awarded so that anti-money laundering supervisors can request SARs from regulated entities. They are also required to report inconsistencies in names, dates of birth, nationalities, etc.

473. **Office of Communications (Ofcom)**[352] – Ofcom oversees telecoms, broadcasting, postal services and online platforms. It ensures compliance with the Broadcasting Act 1996, Human Rights Act 1998 (particularly freedom of expression in Article 10), Communications Act 2003, Online Safety Act 2023 and, most recently, Data (Use and Access) Act 2025.

474. **Information Commissioner's Office (ICO)**[353] – The ICO oversees the processing of data across all sectors, and compliance with data protection principles. The underlying legislation for the ICO's governance is the UK GDPR (General Data Protection Regulation), Data Protection Act 2018, Privacy and Electronic Communications Regulations (PECR), and Data (Use and Access) Act 2025.

475. **Competition Markets Authority (CMA)**[354] – The CMA is the principal authority overseeing compliance with competition law and consumer protection legislation. The CMA enforces the Enterprise Act 2002, Competition Act 1998, Consumer Rights Act 2015, and most recently, Digital Markets, Competition and Consumers Act 2024.

476. **HMRC**[355] – HMRC is the UK's tax, payments and customs authority. It supports, regulates and enforces compliance with tax laws including Income Tax, Corporation Tax,

---

351 Financial Conduct Authority, *Roles and responsibilities in payments regulation*, (2025), [Accessed 19 October 2025].
352 Ofcom, [Accessed 31 September 2025].
353 Information Commissioner's Office, [Accessed 31 September 2025].
354 Competition & Markets Authority, [Accessed 31 September 2025].
355 HM Customs & Revenue, [Accessed 31 September 2025].

VAT, Excise Duties, and Customs Regulations. HMRC ensures compliance with legislation such as the Commissioners for Revenue and Customs Act 2005, Finance Acts, and Money Laundering Regulations 2017. It also supervises anti-money laundering compliance for certain sectors.

477. Unlike many regulators, both the CMA and HMRC have powers to investigate and refer criminal cases for prosecution, with the CMA able to prosecute certain offences directly and HMRC working in partnership with prosecuting authorities.

Barriers to Effective Data-Sharing

478. Having outlined both the existing legislative framework and the regulators, I turn to examine the barriers inhibiting a more proactive approach from both public and private agencies. I identify five key challenges relating to privacy, market competition, collusion risks, concern over tipping off, and cost of compliance.

Protection of Privacy

479. There is a well-established right to privacy for individuals which has been enshrined in the GDPR, the Data Protection Act 2018 and the Human Rights Act 1998. This right to privacy gives individuals control over their digital footprint and shelters them from unwanted abuse, such as potential identity theft. However, in conversation with stakeholders across both the public and private sector, there appears to be considerable confusion over what can be shared without breaching GDPR or the Data Protection Act.

480. Actors in the private sector have detailed their concerns of running afoul of these regulations and facing penalties by the relevant regulatory body. The ICO, for example, can issue fines for serious breaches of data-protection principles, with the maximum penalty reaching £17.5 million or 4% of global turnover.[356]

481. However, it is worth stressing that article (1) e & f specifically note that the processing and sharing of personal data is permitted in cases of 'the public interest'. The Data Protection Act, Article 9 (2), builds upon the GDPR to specifically state: "processing [sensitive personal data as defined by Article 9 (1)] is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject."

[356] Information Commissioner's Office, 'Penalties' [Accessed 31 September 2025].

482. In a statement issued last year, the ICO has stressed that "data protection is not an excuse" to avoid the sharing of data that may prevent fraudulent activity.[357]

Case Study – Equifax Ltd Data Breach[358]

In October 2023, Equifax was fined £11.1 million by the FCA for failures that resulted in it failing to prevent a data breach affecting 13.8 million UK consumers. Equifax had outsourced UK consumer data to its US parent for processing but failed to comply with regulatory requirements for the management of this outsourcing arrangement—meaning that there were no proper oversight, and key vulnerabilities were ignored. The data breach was found to be entirely preventable, and Equifax was also shown to have made misleading public statements about the number of UK consumers affected.

Case Study – Disclosure[359]

Public reporting and academic commentary in the late-1990s to mid-2000s suggested that opportunities for inter-agency information sharing may have been missed in complex fraud/terrorist-finance investigations. These claims have been contested, and the underlying characterisations remain disputed; however, it is possible inter-agency information sharing may have increased the chance that individuals such as Shahzad Tanweer (one of the perpetrators of the 2005 London bombings) could have been identified at an earlier stage.

Press coverage reported that a network associated with Tanweer allegedly gained about £8 billion through VAT and benefit fraud and remitted c. 1% (£80 million) to al-Qaeda. These are reported allegations, not judicial findings, and should be treated with appropriate caution.

This historic case study is illustrative rather than determinative. Its value lies in highlighting the enduring importance of:

a. Clear statutory gateways for lawful disclosure.

b. Coordination of mandates across agencies.

c. Timely, proportionate sharing under documented safeguards.

[357] Information Commissioner's Office, 'Data protection is not an excuse when tackling scams and fraud', news release, 22 November 2024.
[358] Financial Conduct Authority, Financial watchdog fines Equifax Ltd £11 million for role in one of the largest cyber security breaches in history, press release, 13 October 2023.
[359] Ryder, N. and Bourton, S., 'To exchange or not to exchange – that is the question. A critical analysis of the use of financial intelligence and the exchange of information in the United Kingdom', (2023), *Journal of Business Law*, vol. 3, pp. 237–261 [Accessed 30 September 2025].

483. It should be noted that the UK's Data (Use and Access) Act 2025 aims to address some privacy concerns related to data-sharing and access while also promoting innovation and economic growth. It seeks to establish a framework that balances the secure sharing of customer data with appropriate safeguards to protect individuals' privacy. However, this is in the early stage of implementation and does not yet provide a unified mechanism for mapping or integrating fraud data across systems.

Market Competition

484. The second aspect we should consider is the impact of data-sharing. Whilst for financial institutions there is a clear incentive to share data and prevent fraud, as they are obligated to reimburse victims, this incentive is not applicable to other industries.

485. For other sectors, the sharing of personal data may be disadvantageous to firms as it would enable competitors to gain an understanding of their clients and specifically target them. There is also concern that any data shared by companies could be used to train artificial intelligence (AI) models, which can then be commercialised and sold to third parties, including competitors.

486. Alternatively, firms may exploit a fraud committed against their competitors by highlighting the incident to cause reputational damage.

Prevention of Collusion

487. Finally, there is a counter-intuitive concern that data-sharing could be harmful to the competitiveness of markets, as it may enable competitors to share information and engage in collusion and price fixing.

Concern Over Tipping Off

488. Section 333A POCA creates an offence of 'tipping off' if a person in the anti-money laundering regulated sector discloses any matter featuring in a suspicious activity report and it is considered that the disclosure is likely to prejudice an investigation.

489. Additionally, section 342 of the Proceeds of Crime Act 2002 (POCA) makes it an offence to make a disclosure which is likely to prejudice a civil recovery or money-laundering investigation (among others).

490. Both are important offences designed to preserve the integrity of future investigations. However, when the scope of these offences is not properly understood, it can serve as a barrier to businesses disclosing data, even though the overall objective is to detect and disrupt fraud.

Cost of Compliance

491. Lastly, one also needs to consider the cost of compliance with any data-sharing scheme. By its nature, this disadvantages smaller firms who may not have the resources to participate. The cost considerations include:

a. Legal costs to ensure compliance with data protection legislation.

b. Technical and operational costs to develop the systems through which to share data and to build interlinkages with existing system.

c. Administrative costs to develop the business case and to document and oversee the development of the data-sharing project.

d. Membership or data acquisition costs to join existing groups or to bring in external data in addition to the data-sharing scheme.

492. When one considers existing asymmetries between small and large firms, data-sharing may compound disparities and allow larger firms an unfair advantage as they have the resources to gather more data.

International Data-Sharing

493. Having outlined the key concerns constraining voluntary data-sharing, it is important to stress that international actors are not immune from these concerns. The foundational challenge is that there is not a cohesive international framework governing data-sharing across all jurisdictions. Instead, what exists is a patchwork of bilateral and multilateral agreements which countries enter on a voluntary basis. This presents a lack of legal certainty which impedes transnational data-sharing.

494. As fraud is a transnational threat, it is essential that law enforcement agencies can work with public and private sector organisations across borders to complete an intelligence picture and to tackle fraud at its source.

495. This challenge of international data-sharing cannot be divorced from the fraught subject of State sovereignty. The principles of data governance vary from region to region and often closely align with a country's or bloc's cultural values.[360] The European Union's (EU's) GDPR, which is binding on European member states, frames data protection as being underpinned by a fundamental right to privacy, whereas in the United States of America (US) personal data is regarded as a commodity.[361] The principles governing data-sharing in the US are therefore focused on ensuring fairness in the exchange of personal

360 Peterson-Sharma, J., 'The Confusing World of International Data Privacy Law: An Argument for Comprehensive Regulation', *Michigan Journal of International Law*, November 2022.
361 Ibid.

data. International data-sharing agreements can therefore be difficult in that it requires one (or multiple parties) to settle on an agreed process which aligns with their principles.

496. Despite this, there is a growing consensus over the GDPR framework, with many scholars arguing that it is effectively operating as a de facto source of international regulatory standards on data privacy.[362] Japan became the first country on the EU's 'white list' for data-sharing with non-EU countries. An agreement was reached following recognition of the adequacy of Japan's standards. As of March 2025, there are 16 countries on this white list, including the UK.

497. There is a rich academic discussion on why the EU has been able to transpose its data-standard upon the world at large. Undoubtedly, the importance of the European consumer market plays a role as well as elasticity of the EU standards. GDPR is flexible enough for countries to accommodate the regulation alongside their domestic laws and to permit for domestic variations.

498. The UK's departure from the EU raised concerns over the Government's willingness to comply with European standards. Under part 3 of the Trade and Cooperation Agreement (2020) (TCA), UK law enforcement lost access to certain European data-sharing tools but maintained a cooperative framework to share data with member states.[363] However, the TCA is clear that "cooperation may be terminated if the UK is not compliant domestically with the rights and freedoms listed in the European Convention of Human Rights (ECHR) and if the UK shows deficiencies in the protection of sensitive data".[364]

499. Both GDPR and ECHR are already reflected within the UK's domestic legislation, but cooperation remains contingent on the EU's evaluation of the adequacy of the UK's data protection framework. In June 2021, the EU commission published two adequacy decisions assessing the UK's standards as adequate. However, these decisions lasted until 27 December 2025.[365] This date reflects a six-month extension to the original end date to allow the commission to assess the UK's new Data (Use and Access) Act.

500. Beyond the data-sharing with EU member states, the UK has sought to bolster international data-sharing through initiatives such as the Crime and Policing Bill (2025), which allows law enforcement to establish information-sharing agreements via regulations, as opposed to primary legislation.[366] This initiative stands alongside others such as the International Law Enforcement Alerts Platform (I-LEAP).[367] I-LEAP

[362] Schwartz P. M., *Global Data Privacy: The EU Way*, (2019).
[363] Sinardi, M., 'Shared Threats, Divided Laws: The Post-Brexit Future of UK–EU Crime and Data Cooperation', Euro Prospects,18 May 2025.
[364] Ibid.
[365] Information Commissioner's Office, *Adequacy*, (2025), [Accessed 1 October 2025].
[366] Home Office and Ministry of Justice, *Crime and Policing Bill: international cooperation factsheet*, (2025), [Accessed 1 October 2025].
[367] Home Office, *International Law Enforcement Alerts Platform (I-LEAP) Programme Accounting Officer Assessment*, (2023), [Accessed 1 October 2025].

provides a digital platform enabling UK law enforcement, and eventually their equivalent in partnering countries, to access real-time alerts and data from the International Criminal Police Organization (Interpol).

501. Additionally, the UK has taken a leading role in supporting multilateral conventions such as the Budapest Convention on Cybercrime, which provides a framework for international cooperation in investigating and prosecuting cybercrime.[368]

502. The UK has also sought to establish bilateral agreements such as the UK–US Cloud Act agreement (2019), which permits law enforcement agencies from both countries to directly request digital information from technology companies in the other country, bypassing traditional mutual legal assistance (MLA) processes.[369]

503. The UK's current MLA arrangements span a wide consortium of countries, including partners within the Council of Europe Convention, Commonwealth countries, and EU member states. The MLA process enables UK law enforcement to request material from cooperative jurisdictions. However, I have heard concerns that the process is cumbersome and can often slow the process down by months or even years.

504. MLA requests must be issued by a court or a designated prosecuting authority and are ordinarily coordinated through the UK Central Authority (UKCA). In criminal matters, this includes the CPS. HMRC does not bypass this process for MLA; instead, it may use alternative mechanisms, such as Mutual Administrative Assistance ('police-to-police' enquiries) or bilateral arrangements under Double Taxation Conventions (DTA) and Tax Information Exchange Agreements (TIEA), to obtain information from overseas jurisdictions. These routes, however, are primarily designed for civil tax inquiries and may not always meet evidential standards for criminal proceedings.[370]

505. Furthermore, investigative forces have noted that the process can be cumbersome, and that requesting material can delay proceedings significantly. In a later chapter, 'Powers', below, I consider the limitations on UK law enforcement to compel information from foreign entities.

Recommendations

506. Through extensive engagement with both public bodies and private sector organisations, it has become evident that the legal infrastructure for data-sharing, though broadly in place, is frequently underutilised, misunderstood, or inconsistently applied. It is of particular concern that an enforcement authority may feel unable to share information

---

[368] Council of Europe, 'The Convention on Cybercrime (Budapest Convention, ETS No. 185) and its Protocols', [Accessed 1 October 2025].

[369] U.S. Department of Justice, 'U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online', press release, 3 October 2019, [Accessed 1 October 2025].

[370] I consider MLAs in greater depth within the chapter 'Powers'.

with another authority even if that information could assist in identifying fraud. This fragmented landscape undermines the speed and effectiveness with which fraud can be detected, investigated and prosecuted.

507. Data-sharing is not a peripheral technicality; it is central to the integrity and operational efficacy of the criminal justice system. As fraud becomes increasingly complex and digitally enabled, our response must evolve accordingly. That evolution does not begin with new legislation, but with leadership, clarity, and a shared commitment to using existing powers lawfully, confidently and effectively. There are two distinct but complementary tracks for reform.

508. **Track One – Immediate Clarifications Within the Existing Framework.** In the short term, there is a pressing need to clarify and simplify the current data-sharing landscape. This includes improving awareness of existing powers, streamlining operational guidance, and removing unnecessary procedural barriers.

Recommendation 11

Until a statutory framework has been created, establish a single memorandum of understanding between public bodies setting out how data and intelligence can be shared between these agencies, for the purpose of detecting and investigating fraud.

Recommendation 12

a. The Home Office, working with the National Crime Agency (NCA) and Information Commissioner's Office, should provide guidance on voluntary and compelled data-sharing for public and private sector organisations, drawing upon section 7 of the Crime and Courts Act 2013, regulation 103(1) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, and the Economic Crime and Corporate Transparency Act 2023. This should explicitly cover information sharing between private sector organisations, setting out the legal basis and safeguards.

b. The Government should clarify the scope of sections 333 and 342 of the Proceeds of Crime Act 2002 concerning the tipping off offence and the prejudicing of an investigation. The NCA should provide assurance that, where information is shared with the objective being to combat criminal activity in line with this guidance, these provisions will not apply.

509. Further, current provisions under Section 3 of the Criminal Justice Act 1987 allow the SFO to share information with Government departments, but the scope is narrow and lacks the flexibility required to tackle modern economic crime. By contrast, Section 7 of

the Crime and Courts Act 2013 operates as a gateway for any person,[371] such as an individual, private organisation or another enforcement authority like HMRC, to share intelligence with the NCA, enabling faster and more integrated enforcement.

510. This provision entered into force on 7 October 2013 and also facilitates the NCA's sharing of information with others. In an era of complex, digitally enabled fraud, the SFO should be equipped with equivalent powers to exchange information confidently and lawfully across agencies. Aligning Section 3 with the Crime and Courts Act model would remove unnecessary barriers, strengthen inter-agency collaboration, and ensure that intelligence flows keep pace with the speed and sophistication of criminal networks.

Recommendation 13

Section 3 of the Criminal Justice Act 1987 should be amended to mirror the information gateway in Section 7 of the Crime and Courts Act 2013, thereby enabling the Serious Fraud Office to share and receive information with greater flexibility and operational reach.

511. **Track Two – Structural Reform of the Legislative and Operational Framework.** Arguably more important is the need for a fundamental review of the legislative architecture governing data-sharing. The current framework, comprising a patchwork of statutory provisions, memorandums of understanding and bilateral agreements, is ill-suited to the demands of modern fraud and economic crime investigation.

Recommendation 14

The Government to conduct a comprehensive review of the data-sharing provisions and arrangements to enable the detection and investigation of fraud. This should include sharing within and between the public and private sectors.

Further Government Initiatives

512. Streamlining the data-sharing provisions will be vital for new initiatives such as the proposed Online Crime Centre. This multi-agency and public private capability, led by City of London Police, the NCA and the National Economic Crime Centre, will be dependent on robust and legally sound intelligence-sharing pathways.[372]

513. Additionally, the Home Office is also considering plans to establish an Economic Crime Data Advisory Hub, which will maintain an overall view of data-sharing initiatives, with

[371] Other than persons in the Security Service, Secret Intelligence Service or GCHQ.
[372] This is discussed further in the chapter 'Detection and Disruption'.

the ability to accelerate and coordinate priority projects. The hub will be tasked with the following priorities:

a. Ensure implementation of the strategy commitments through monitoring and evaluating delivery of the actions.

b. Raise awareness in the public and private sectors regarding how data can be shared for tackling economic crime purposes.

c. Support new data-sharing initiatives through the provision of specialist expertise.

d. Identify how data-sharing initiatives and capabilities can be better joined up to make the overall economic crime data system more effective and efficient.

514. In addition to these initiatives, the Government has announced the introduction of mandatory digital IDs. I have discussed this subject in greater detail in the chapter on emerging threats, but it is worth repeating that, whilst this technology could greatly improve data-sharing across financial services, reducing the cost of compliance and reduce reliance on easily forged documents, mandatory digital IDs are not without their risks. Such a system must be underpinned by rigorous verification and anti-tampering safeguards, and those developing it should be mindful of potential mission creep.

Conclusion

515. Data-sharing is not an end in itself. It is a means by which agencies and organisations pursue broader public interest goals, protecting victims, disrupting criminal networks and upholding the rule of law. As the world becomes ever more digital, we must ensure that our data-sharing framework is fit for purpose: clear, lawful, and capable of supporting the swift and effective pursuit of fraudsters at home and abroad.

516. Whilst the current initiatives are a step in the right direction, it remains essential that the framework for data-sharing is easily understood by all parties, protects individuals' privacy, and safeguards against future threats.

11. Whistleblower Incentivisation

517. Having considered the State's access to bulk data and systemic intelligence through public–private partnerships, tools essential for mapping the fraud threat at scale, I now turn to a narrower but no less critical domain: case-specific intelligence. In serious and complex fraud investigations, the law enforcement agencies are not merely scanning the horizon; they are searching for a direct route into the heart of criminal fraudulent activity. One route is through structured partnerships with multinational firms. Another, more direct, is through individuals, those with inside knowledge and the courage to speak up. Whistleblowers, in this context, are not peripheral actors. They are potential catalysts for enforcement.

518. Moreover, it is not disputed that the detection of serious and complex economic crime, including fraud, bribery, and corruption, is more efficient when authorities are provided an inside track to possible offending. The United Kingdom (UK), however, has long wrestled with the idea of law enforcement agencies paying whistleblowers for information, going further than current accepted practices of paying Covert Human Intelligence Sources. It is argued that, in part, this reluctance is due to a cultural aversion to 'telling tales', looking down upon those who go to the authorities behind the back of a neighbour, colleague or business partner.

519. More recently, the whistleblowing debate, particularly with regard to economic crime, has shifted. The National Crime Agency (NCA) assesses that fraud and money laundering cost the UK economy a combined total of £290 billion a year, whilst others estimate the cost of all economic crime could be anywhere up to £350 billion per year.[373] The impact of this criminality extends beyond individual and corporate victims, inflicting damage on the UK economy as a whole.

520. Over the last year, UK law enforcement agencies have sought to highlight the success of the United States of America's (US) whistleblower incentivisation programmes in assisting the detection and enforcement of such criminality. Led by the Serious Fraud Office (SFO),[374] this call for reform has prompted renewed discussion around the concept of rewarding whistleblowers and whether financial incentivisation has a role to play in the detection, investigation and prosecution of economic crime in the UK.

521. In parallel, the Royal United Services Institute (RUSI) published a research paper on whistleblowing incentivisation in December 2024. The report examined the role of rewards for whistleblowers in the fight against economic crime, analysing evidence from

---

[373] APPG for Anti-Corruption & Responsible Tax and UK Anti-Corruption Coalition, *Clean Foundations For Growth: Unlocking Economic Opportunity by Tackling Economic Crime*, (2025), [Accessed 9 July 2025].
[374] Serious Fraud Office, *Annual Report and Accounts 2024-25,* (2025), pages 13 and 50.

reward programmes in the US and Canada to make key observations applicable to countries exploring the concept, such as the UK.[375]

522. The argument for the introduction of incentivisation is multi-faceted. Firstly, it is postulated that the UK is experiencing a drain of information as whistleblowers are opting to disclose to US agencies where they could be rewarded millions of dollars for their contribution. Spotlight on Corruption estimated that UK whistleblowers are the second-largest users of US whistleblower programmes, with 774 UK nationals giving tips to the four different US programmes between 2012 and 2023.[376]

523. Secondly, law enforcement agencies assess that whistleblower incentivisation could help to increase the speed of economic crime investigations. Without insider information to assist the detection of crime, UK law enforcement agencies must start from scratch in complex cases which often have a transnational element. These investigations are lengthy, over the past three years, the average time from opening an SFO investigation to first resolution (i.e. charge) has been approximately 4.3 years.[377] The SFO suggests that, if it had access to inside information, it could likely focus investigations at an earlier date, leading to a timelier resolution. Given the current backlog of over 76,000 cases in the Crown Court,[378] resulting in an average of approximately 2.5 years between charging decision and commencement of an SFO trial,[379] there is understandably an appetite from some agencies to speed up the process.

524. The first two arguments pertain to benefits seen by UK law enforcement; the third argument I have encountered is the proposed potential improvement to corporate culture. It has been suggested that the introduction of whistleblower incentivisation may further encourage corporates to rigorously investigate reported wrongdoing, in the knowledge that employees could otherwise take concerns regarding possible criminal activity to an agency. By implementing robust safeguards and internal reporting channels for fraud, bribery and corruption, corporates can reduce the risk of an external whistleblower-facilitated investigation.

525. Conversely, I have heard concerns that a whistleblowing regime could encourage a proliferation of false and malicious reports. There are also criticisms of the State's inability to adequately protect real whistleblowers from retaliation, some of whom will need substantial support for the rest of their lives. I will consider these issues, and others, in more detail later in this chapter.

---

375 Lockhart, E., *The Inside Track: The Role of Financial Rewards for Whistleblowers in the Fight Against Economic Crime*, Serious Organised Crime & Anti-Corruption Evidence Research Programme, (2024).
376 Hawley, S. and Davis, M., '[Time for a rethink on whistleblower compensation in the UK to fight economic crime?]', Spotlight on Corruption, 12 March 2023. [Accessed 26 June 2025].
377 Statistic provided by Serious Fraud Office.
378 Ministry of Justice, *Criminal court statistics quarterly: January to March 2025*, chapter 5.1.
379 Statistic provided by the Serious Fraud Office. This average is based on records taken over the past three years.

526. In light of the above, I feel it is the right time to re-evaluate whether whistleblower incentivisation could be a useful tool to help progress the detection, investigation and prosecution of serious economic crime and fraud, to foster a greater corporate resilience to such crime in the UK.

Definitions

527. Before examining the arguments, I have set out definitions for the different types of individuals who provide information to UK law enforcement. For the purpose of this Review, the term 'whistleblower' will be defined in its broadest sense, as a worker who exposes wrongdoing within an organisation. Taking a narrower view, a whistleblower is defined as someone who discloses information in order to report and correct corruption.[380]

528. Whistleblowers are currently protected under the Public Interest Disclosure Act 1998.[381] To be covered by whistleblowing law, an employee who makes a disclosure must reasonably believe two things:

a. That they are acting in the public interest.

b. That the disclosure tends to show past, present or likely future wrongdoing falling into one or more of the following categories: criminal offences, failure to comply with an obligation set out in law, miscarriages of justice, endangering of someone's health and safety, damage to the environment, or covering up wrongdoing in the above categories.[382]

529. Alongside whistleblowers, there are other individuals who can provide information exposing wrongdoing. I have set these out below.

530. **Covert Human Intelligence Source (CHIS)** – A person who is authorised under the Regulation of Investigatory Powers Act 2000[383] to establish or maintain a personal or other relationship to covertly gather information on behalf of law enforcement or the security services. A CHIS may be a police officer, an individual holding a position in a public authority who is acting undercover, or a member of the public recruited by a public authority.[384]

531. **Assisting Offender** – An offender who provides intelligence and/or evidence to an investigation and prosecution about the criminal activity of other defendants. In exchange for their cooperation, assisting offenders may receive a reduced sentence or immunity

[380] Schultz, D. and Harutyunyan, K., 'Combating corruption: The development of whistleblowing laws in the United States, Europe, and Armenia', *International Comparative Jurisprudence*, vol. 1, no. 2, 2015, pp. 87–97.
[381] Public Interest Disclosure Act 1998.
[382] Ibid, s.1.
[383] Regulation of Investigatory Powers Act 2000.
[384] Ibid, s.26.

from prosecution.[385] The legislative framework for assisting offenders is provided by the Serious Organised Crime and Police Act 2005[386] and Sentencing Act 2020.[387]

532. **Informant** – A person who gives information to another person or organisation.[388] This term is commonly used among the law-enforcement community to describe an individual who provides information relating to criminality; however, it has no legal footing. The Metropolitan Police stated in a recent Freedom of Information request response that it now avoids using this term, to prevent confusion.[389]

Jurisdictions Utilising Whistleblower Rewards

533. Whilst the UK has long debated the efficacy of formally financially rewarding whistleblowers in economic crime cases, other jurisdictions have wholeheartedly embraced the concept. I believe there is value in exploring international models of whistleblowing, before considering if the UK can learn from these regimes, while remaining cognisant of the fundamental differences between each jurisdiction's enforcement and justice systems.

United States

534. The US is often cited as a leading example in this field, with a number of sophisticated whistleblower incentivisation schemes in place, and it must be noted that, unlike in the UK, it is not essential that a whistleblower works for the organisation they are reporting.[390] The False Claims Act 1863 (modernised in 1986) is the oldest US whistleblower reward scheme. For economic crime specifically, there are four major reward programmes operated by the Internal Revenue Service, Securities Exchange Commission, Commodity Futures Trading Commission, and Department of the Treasury's Financial Crimes Enforcement Network. More recently, the Department of Justice (DoJ) launched a whistleblower reward programme targeting significant corporate or financial misconduct.

535. **The False Claims Act 1863**, administered by the DoJ, provides the oldest whistleblower reward programme in the US. The Act allows private individuals to bring *qui tam*[391] actions against private parties relating to fraud against the US government. If the action is successful, the whistleblower keeps a portion of any proceeds which are otherwise returned to the US government's federal treasury. In 1986, following previous amendments, the Act was further amended to include retaliation protections, to increase

385 Crown Prosecution Service, 'Assistance provided by Offenders', [Accessed 22 September 2025].
386 Serious Organised Crime and Police Act 2005.
387 Sentencing Act 2020.
388 Cambridge Dictionary, Informant | English meaning, [Accessed 11 September 2025].
389 Metropolitan Police, *Covert Human Intelligence Source data since 2015*, [Accessed 14 September 2025].
390 National Whistleblower Center, 'What is a whistleblower?', [Accessed 9 August 2025].
391 Legal Information Institute, 'qui tam action', [Accessed 2 July 2025]. In a *qui tam* action, a relator brings an action against a person or company on the government's behalf. The government, not the relator, is considered the plaintiff. If the government succeeds, the relator bringing the suit receives a share of the award.

the maximum reward to 30% of the sum recovered and to restrict the payment of awards to whistleblowers involved in the criminal conduct.

536. **The Internal Revenue Service (IRS) whistleblower programme** was created by amendments to the Tax Relief and Health Care Act of 2006.[392] Under this programme, whistleblowers who report tax problems in their workplace or elsewhere can be awarded between 15% and 30% of the total amount the IRS recovers, provided it is greater than US $2 million. The Whistleblower Office is responsible for assessing incoming tips and determining their credibility.[393] Each financial year, the Office publishes an annual report to Congress on the results of the scheme, programme developments, and legislative and administrative recommendations.[394]

Case Study – Bradley Birkenfeld and UBS

It was under the IRS programme that Bradley Birkenfeld was awarded US $104 million for blowing the whistle on a tax evasion scheme at the Swiss bank UBS.[395] Birkenfeld was a former wealth manager at UBS and, alongside receiving a significant reward for his tip, he was also convicted by the DoJ for his involvement in the criminality, receiving a 40-month jail sentence. This case is seen as a shift in US tax enforcement, following which the IRS saw an increase in self-reports and participation with their whistleblower programme, which led to over US $11 billion being collected in back taxes and the prosecution of several banks.

537. **The Securities and Exchange Commission (SEC) whistleblower programme** was implemented under the Dodd–Frank Wall Street Reform and Consumer Protection Act 2010[396] (the Dodd–Frank Act). The SEC programme provides financial rewards for whistleblowers who report federal securities laws violations which result in monetary sanctions of over US $1 million.[397] Individuals who provide original information which leads to successful enforcement action are entitled to between 10% and 30% of the monetary sanctions imposed, with discretion afforded to the SEC as to where an award should fall within those thresholds. The SEC produces an annual report on the total amount of rewards paid and number of individuals who received awards, in 2024, over US $255 million was awarded to 47 individuals.[398]

---

392 Tax Relief and Health Care Act of 2006.

393 Internal Revenue Service, 'Whistleblower Office at a glance', [Accessed 2 July 2025].

394 Internal Revenue Service, *IRS Whistleblower Office Fiscal Year 2024 Annual Report*, (2024).

395 Kohn, Kohn & Colapinto LLP, *UBS Insider Blows Open Swiss Banking Secrecy*, [Accessed 2 July 2025].

396 Dodd–Frank Wall Street Reform and Consumer Protection Act 2010.

397 U.S. Securities and Exchange Commission, 'Whistleblower Program: Frequently Asked Questions', [Accessed 2 July 2025].

398 U.S. Securities and Exchange Commission Office of the Whistleblower, *Annual Report to Congress for Fiscal Year 2024*, (2024), page 1.

538. **The Commodity Futures Trading Commission (CFTC) whistleblower programme** was also established under the Dodd–Frank Act. This programme provides financial incentives to individuals reporting potential violations of the Commodity Exchange Act 1936.[399] To be eligible for an award, the whistleblower's tip must lead to the CFTC carrying out successful enforcement action which results in monetary sanctions of at least US $1 million. Eligible whistleblowers can receive an award of between 10% and 30% of the amount of monetary sanction collected.

539. The programme aims to provide whistleblowers with privacy, confidentiality and anti-retaliation protections. The CFTC made its first award to a whistleblower in 2014 and since then has awarded approximately US $390 million to whistleblowers. Associated enforcement actions have resulted in over US $3.2 billion being recovered by the CFTC.[400]

540. **The Financial Crimes Enforcement Network (FinCEN)** is a division in the US Department of Treasury. Under the Anti-Money Laundering Act 2020[401] the FinCEN whistleblower programme was established for individuals to report breaches of the Anti-Money Laundering Act, Bank Secrecy Act[402] or sanctions violations. Whistleblowers are eligible for an award of between 10% and 30% of the penalties and fines obtained by FinCEN if the penalties and fines exceed US $1 million.[403]

541. **The Department of Justice Pilot Programme** was launched in 2024 to "discover significant corporate or financial misconduct". The pilot was modelled on the SEC, CFTC and FinCEN programmes in order to seek information regarding corporate misconduct that is not within scope of the existing programmes. Individuals reporting original and truthful information regarding corporate misconduct may be eligible to receive a percentage of the forfeited assets, should their report lead to a successful forfeiture.

542. Under each of the US programmes, it is the responsibility of the rewarding agency to determine a whistleblower's eligibility and size of the reward paid. Each agency has an Office of the Whistleblower function which acts as the decision maker for such matters, among other roles.[404]

---

399 Commodity Exchange Act 1936.

400 Commodity Futures Trading Commission, *The Whistleblower Program*, [Accessed 2 July 2025].

401 Anti-Money Laundering Act 2020.

402 Bank Secrecy Act.

403 Whistleblower Partners LLP, 'FinCEN Whistleblower Program', [Accessed 2 July 2025].

404 Lockhart, E., *The Inside Track: The Role of Financial Rewards for Whistleblowers in the Fight Against Economic Crime*, Serious Organised Crime & Anti-Corruption Evidence Research Programme, (2024).

Other Jurisdictions

543. Whilst the US is recognised as running the most advanced incentivisation programmes, it is worth noting that there are other jurisdictions also utilising financial rewards.

544. **Canada's Revenue Agency (CRA)** established the country's first whistleblower reward programme in 2014, under the Offshore Tax Informant Program. This programme rewards whistleblowers who report international tax non-compliance. If the information provided results in the collection of at least CAD $100,000, the whistleblower becomes eligible for between 5% and 15% of the additional federal tax collected.[405] By 2019, CAD $19.3 million had been collected by the agency in federal taxes and over CAD $1million of rewards had been paid to whistleblowers.[406]

545. **The Ontario Securities Commission (OSC)** followed suit and in 2016 passed its own whistleblower programme. This programme offers whistleblowers protection and reward of up to CAD $5 million for tips on violations of Ontario securities law that lead to enforcement action. Between 2016 and 2022 more than CAD $9 million was paid to 11 whistleblowers.[407]

546. Despite operating on a smaller scale than US models, both the CRA and OSC appear to have had success in encouraging the sharing of useful information by whistleblowers.

547. **South Korea's National Tax Service** operates a tax evasion informant reward programme and Foreign Financial Account Report Reward Programme, both of which are designed to encourage individuals to bring forward information leading to successful tax enforcement action. If an individual reports significant information relating to tax evasion, they could receive an award of between 5% and 20% of the money recovered. Individuals reporting under the foreign financial account programme could be eligible to receive between 5% and 15% of the collected sanctions.[408]

548. **South Korea's Anti-Corruption and Civil Rights Commission** also runs a whistleblower reward programme for reports of public sector corruption. Individuals can be financially rewarded for providing reports that directly lead to recovering or increasing revenue for central or local government, or if the information enhances public interest.[409]

549. Given the plethora of models established by other jurisdictions, it is clear that incentivisation schemes must be designed to target specific criminality and a 'one-size-fits-all' model is not sufficient. It is also important to note that the models outlined above

---

405 National Whistleblower Center, 'Canadian Whistleblower Reward Laws', [Accessed 9 July 2025].
406 Sorensen, M. and Arrigo, N., 'Whistleblowing Pays Off—New CRA Data on First Payments to Informants', blog, Bennett Jones, 21 August 2019.
407 Ontario Securities Commission, *Update on the OSC Whistleblower Program 2016 to 2022*, (2023).
408 Republic of Korea National Tax Service, *Tax Whistleblower Reward Program*, [Accessed 9 July 2025].
409 Anti-Corruption & Civil Rights Commission (Korea), 'Punishment & Detection Policy', [Accessed 9 July 2025].

are not without their drawbacks. Critics highlight that, under some US programmes, fewer than 1% of whistleblowers who make a disclosure receive a financial reward. In 2023, despite receiving over 18,000 tips, the SEC paid awards to only 68 individuals.[410] This triggers concerns around reward expectation management and the uneven distribution of benefits, with only a small number of individuals receiving the bulk of financial rewards. Questions have also arisen around whether incentivisation schemes are truly effective at driving high-quality reports, given that so few reports lead to a reward. Are agencies instead swamped with frivolous or low-quality disclosures?

550. It has become clear to me that overseas jurisdictions find value in whistleblower incentivisation to encourage the provision of information to detect crime. The US, Canada and South Korea have all reported high numbers of tips being received by enforcement agencies, some of which have led to successful enforcement action. There will undoubtedly be valuable lessons that the UK can learn, and relevant comparisons to make with those jurisdictions who financially reward whistleblowers.

The UK Landscape

551. Whilst the UK does not have incentivisation schemes operating on the same scale of those in the US, the concept of the State paying an individual for the provision of information is not a new one. In fact, there have been multiple Acts of Parliament since at least 1575 dealing with common informers. Where statute permitted, and for certain offences, any individual could pursue a person suspected of wrongdoing themselves, and in return would receive a proportion of any penalty or forfeiture which resulted from the legal action. Much later, the Common Informers Act 1951 abolished the ability of a common informer to bring proceedings in which they would receive some of the penalty or forfeiture arising from the proceedings.[411]

552. For a number of years, police forces have also provided payment to individuals authorised as CHIS for participating in the covert investigation of criminality. Whilst it is unclear when this practice began, the authorisation and oversight of CHIS activity was later formalised under the Regulation of Investigatory Powers Act 2000[412] and Covert Human Intelligence Sources (Criminal Conduct) Act 2021.[413]

553. In financial year 2022/23, the Metropolitan Police Service paid a total of £1,041,442.60 for the services of individuals authorised as CHIS.[414] The use and payment of CHIS is now a well-established tactic deployed by police forces. Whilst there are considerable differences between the payment of CHIS and whistleblower incentivisation schemes, it

---

410 U.S. Securities and Exchange Commission Office of the Whistleblower, *Annual Report to Congress for Fiscal Year 2023*, (2023), page 1. The 2024 Report was not used due to concerns regarding the reliability of data included.
411 Common Informers Act 1951 s1.
412 Regulation of Investigatory Powers Act 2000.
413 Covert Human Intelligence Sources (Criminal Conduct) Act 2021.
414 Metropolitan Police Service, *Covert Human Intelligence Source data since 2015*, (2023).

further illustrates the concept of individuals receiving a financial sum for providing information to law enforcement.

554. On a similar note, the SFO's latest annual report indicated that between 1 April 2024 and 31 March 2025 its Intelligence Divisions handled 167 qualifying whistleblowing disclosures. Of these 167 cases, the SFO acted in 153—which could include sending a personalised response, requesting more information and/or making further enquiries with partner agencies.[415]

UK Whistleblower Protections

555. The UK also recognises the need to protect whistleblowers from retaliation by their employers, offering this through the Public Interest Disclosure Act 1998 (PIDA), which is embedded within the Employment Rights Act.

556. While the statute does not use the term 'whistleblower' explicitly, it provides protections for workers who make a 'protected disclosure'. The scope and enforcement of these provisions have been subject to considerable debate, which falls outside the remit of this Review. However, it is essential to stress that any whistleblowing regime can only succeed if individuals feel confident that the protections offered are robust enough to encourage them to come forward. We must recognise the stark disparity in power between lone whistleblowers and large organisations, particularly multinational corporations, whose resources are able to employ high-level law firms to engage in vexatious litigation, creating a chilling effect on those who seek to expose wrongdoing.

557. In June 2025, new provisions under the Economic Crime and Corporate Transparency Act 2023 (ECCTA) came into force to tackle Strategic Litigation Against Public Participation (SLAPP). Section 194 requires the Civil Procedure Rules to include a mechanism to strike out SLAPP claims relating to economic crime prior to trial commencing and introduce cost protections for defendants. Section 195 provides the first statutory definition of a SLAPP claim in the context of economic crime. These provisions provide protection to defendants who expose wrongdoing and find themselves subject to harassment through legal action. By enabling the early dismissal of SLAPPs and limiting cost risks for those subject to such claims, whistleblowers who report economic crime will be encouraged to do so without being unfairly burdened by strategic lawsuits.

Financial Rewards

558. Moving more specifically to reward schemes, there are two UK enforcement agencies operating schemes for individuals providing information; HM Revenue and Customs and the Competition and Markets Authority. It is important to note that neither of these

[415] Serious Fraud Office, *Annual Report and Accounts 2024-25*, (2025), pp. 13 and 50.

schemes are targeted specifically towards whistleblowers as defined by PIDA, rather any individual who provides relevant information.

559. **HM Revenue and Customs (HMRC)** possesses a statutory basis for paying financial rewards for information under the Commissioners for Revenue and Customs Act 2005.[416] This Act established the department as it operates today. Prior to this legislation, the precursor departments, Customs & Excise and Inland Revenue, also had powers to allow the payment of rewards for the provision of information under the Customs and Excise Management Act 1979[417] (now repealed) and Inland Revenue Regulation Act 1890.[418]

The Commissioners for Revenue and Customs Act 2005, section 26

The Commissioners may pay a reward to a person in return for a service which relates to a function of—

(a)the Commissioners, or

(b)an officer of Revenue and Customs.

560. Under section 26, HMRC makes discretionary payments to individuals who report suspected tax fraud. Unlike some international models, the size of the reward is not linked to the amount of tax recovered. Whilst data regarding the payment of rewards is not routinely published by HMRC, in financial year 2023/24, £978,256 was paid to individuals reporting tax evasion, an increase from £508,500 in the previous year.[419]

561. In March 2025, HMRC announced that it will be launching a new reward scheme to run alongside its existing one. The new scheme is modelled on those seen in the US and Canada, with individuals receiving a percentage of tax recovered as a result of their disclosure.[420] This commitment was reaffirmed by the Chancellor of the Exchequer in the November 2025 budget.[421]

562. **The Competition and Markets Authority (CMA)** also publicly acknowledges that it offers financial rewards for information. Individuals providing information relating to cartel activity are eligible for a reward of up to £250,000.[422] Unlike HMRC's, this scheme does not operate on a statutory footing, and rewards are granted under internal policy agreed by the CMA.

---

416 Commissioners for Revenue and Customs Act 2005 s.26.
417 Customs and Excise Management Act 1979 s.165.
418 Inland Revenue Regulation Act 1890 s.32.
419 Park, A., 'Contentious Tax Bulletin November 2024', (2024).
420 Exchequer Secretary to the Treasury, '20 years of HMRC - reflections and looking ahead', speech delivered on 11 March 2025.
421 HM Treasury, *Budget 2025*, (2025), para 3.3.
422 Competition & Markets Authority, *Rewards for information about cartels*, (2014).

563. Though these schemes exist, the debate regarding the efficacy of more formal whistleblower incentivisation in the UK has yet to reach a conclusion. In 2013, the Parliamentary Commission on Banking Standards recommended a review of US incentivisation schemes. Two years later, the Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) jointly published a report responding to this recommendation. The report opposed the concept of whistleblower incentivisation and concluded that it would not encourage people to come forward.[423] A decade later, under new leadership, the FCA's stance may be shifting. In 2024, Nikhil Rathi (Chief Executive of the FCA) stated that, although it would be highly countercultural for the UK to implement US-style schemes, he was not opposed to the idea of remunerating individuals for coming forward.[424]

Non-Financial Rewards

564. Alongside the financial reward landscape, there are other tools on the statute books which aim to encourage the provision of information to assist the detection, investigation and prosecution of criminality including fraud. Such tools relate to reductions in the degree of possible punishment rather than financial rewards. One such example is the assisting offenders regime, operated under the Serious Organised Crime and Police Act 2005[425] (SOCPA) and later amended by the Sentencing Act 2020.[426]

Measures for assisting offenders

Section 71 SOCPA

A specified prosecutor can provide an offender immunity from prosecution for any offence as a result of their cooperation in the investigation or prosecution of an indictable offence or an offence triable either way.

Section 72 SOCPA

The Crown is empowered to issue an undertaking that they will not use an individual's information against them in certain circumstances.

Section 74 Sentencing Act 2020

This measure replaced section 73 SOCPA. It allows for the reduction in sentence for an offender who provides assistance to the prosecution.

423 Financial Conduct Authority and Prudential Regulation Authority, *Financial Incentives for Whistleblowers*, (2014), [Accessed 22 July 2025].
424 *Financial Times*, 'UK should pay whistleblowers to cut financial crime, says think-tank', 8 December 2024, [Accessed 22 July 2025].
425 Serious Organised Crime and Police Act 2005 s.71–75.
426 Sentencing Act 2020 s.74.

565. Whilst these provisions are available to investigators and prosecutors, I understand that they are seldom used. I discuss this point in further detail in a later chapter, 'Penalties'.

<u>US Whistleblower Protections</u>

566. In the US, whistleblower protections are codified across multiple statutes to safeguard individuals from retaliation and ensure confidentiality. The False Claims Act includes robust anti-retaliation provisions, allowing whistleblowers to seek reinstatement, double back pay, and compensation for damages if they suffer adverse employment actions. Similarly, the Dodd–Frank Act expanded protections for those reporting securities law violations to the SEC or CFTC, prohibiting employers from retaliating and granting whistleblowers the right to bring private actions in federal court.

567. Under the Sarbanes–Oxley Act 2002, employees of publicly traded companies who report fraud are protected from dismissal or harassment, with remedies: reinstatement and compensatory damages. These protections are complemented by confidentiality guarantees within the SEC and CFTC programmes, which permit anonymous reporting through legal counsel. Collectively, these measures aim to reduce the chilling effect of employer retaliation and encourage individuals to disclose wrongdoing without fear of reprisal.

568. Beyond statutory safeguards, US agencies operate dedicated Offices of the Whistleblower, which manage claims, enforce anti-retaliation provisions, and provide guidance on rights and remedies. The combination of financial incentives and strong legal protections has been credited with driving high-quality disclosures, though critics note that enforcement of anti-retaliation provisions can be uneven and resource-intensive.

Discussion

569. Having considered the current landscape in detail, I have uncovered a number of arguments both for and against whistleblower incentivisation.

570. **Cultural views** are often cited as a reason to not introduce whistleblower incentivisation schemes to the UK and "it's not British" is a phrase that I have heard several times throughout my engagement. Critics often note that whistleblowers should report criminality because it is their moral duty to do so. Others make reference to the fact that the State should not be paying its citizens for information.

571. I have taken on board the experiences of those jurisdictions more advanced in this space when considering the cultural perception of whistleblowing. RUSI's research points to evidence from the US that suggests a moral duty alone is not enough to encourage whistleblowers to come forward.[427] Similarly, as I have set out in this chapter, the most

[427] Lockhart, E., *The Inside Track: The Role of Financial Rewards for Whistleblowers in the Fight Against Economic Crime*, Serious Organised Crime & Anti-Corruption Evidence Research Programme, (2024), pp. 32–33.

effective incentivisation models seen overseas reward based on outcome; this is a different model to the State paying for information in advance. It is the former that law enforcement agencies such as the SFO have presented to me, and it is important to draw this distinction when considering the efficacy of such a model in the UK.

572. Taking on board the cultural criticisms, I commissioned polling to better understand the public perception of whistleblower incentivisation. The results of the poll in fact show that the majority of respondents were supportive of whistleblowers receiving financial rewards, should their information lead to a successful outcome.

Public Polling – Rewarding Whistleblowers (Ipsos)

<u>Question</u>

A representative sample of adults (2028) aged 16–75 in Great Britain were asked the following:

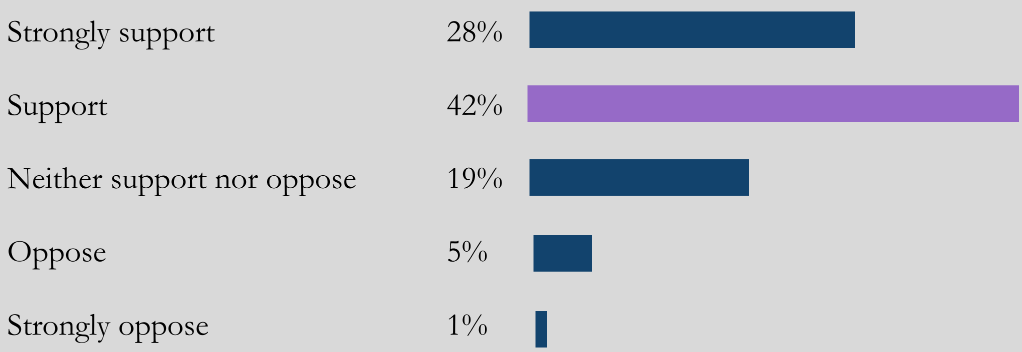
"A whistleblower is a person who reports evidence of economic crime to law enforcement agencies. In the United States, whistleblowers can be financially rewarded for exposing economic crime. Whistleblowers are eligible for a financial reward if their information leads to a successful conviction or guilty plea.

As a reminder, economic crime is a broad category of activity involving money, finance or assets, the purpose of which is to unlawfully obtain a profit or advantage for the perpetrator or cause loss to others. Examples of economic crime include fraud, money laundering, sanctions evasion and corruption.

Would you support or oppose a scheme that financially rewarded whistleblowers in the UK who expose serious economic crime?"

<u>Response</u>

Public sentiment was generally positive, with 70% of participants supporting financially rewarding whistleblowers of serious economic crime.



573. Given that a representative sample of the UK population was polled for this matter, I do not feel that the cultural perception of whistleblower incentivisation is likely to be a barrier to the success of a scheme.

574. **Unintended consequences** of introducing a whistleblower incentivisation scheme have also been raised. The possibility of receiving a financial reward could encourage individuals to submit false or frivolous reports or to provide unreliable evidence in court. In a similar vein, individuals may delay reporting criminality they are aware of in the hope that they will receive a greater reward if the criminality becomes more serious over time. The offer of financial rewards from law enforcement could also encourage whistleblowers to undermine internal reporting mechanisms within their company to report externally instead.

575. Drawing from the experience of the US, it appears that submission of fraudulent information can be managed. The SEC possesses the ability to bar individuals who submit false information or repeatedly make frivolous award claims. A further protection against false or otherwise unreliable submissions is the fact that authorities must successfully bring action based on the information before a reward is given.[428] Additionally, when determining the eligibility of an individual for reward, US authorities take into account the time between the whistleblower becoming aware of the fraud and reporting it, thus providing an incentive for whistleblowers to report wrongdoing at the earliest possible opportunity.[429] If the UK were to introduce a scheme without sufficient guardrails, these concerns could manifest; however, we can see evidence in the US that such issues can be mitigated.

576. I acknowledge the risk that a whistleblower may undermine internal processes to report wrongdoing to law enforcement; however, it is possible that this could also generate positive impacts on corporate culture. If, due to incentivisation, whistleblowers are more likely to report criminality to law enforcement, this increases the risk of a corporate's wrongdoing being exposed. Corporates must ensure that they are complying with the law or make a self-report to law enforcement if they want to avoid a whistleblower-facilitated investigation. Alongside other incentives, such as the SFO's new corporate cooperation guidance,[430] one can imagine that whistleblower incentivisation could shift the corporate cooperation landscape for the better.

577. **Procedural issues** of running a reward programme may also arise, such as managing disputes between a whistleblower and law enforcement, the leak of a whistleblower's information, or diplomatic issues where a whistleblower reports internationally. Whilst these are very real risks, there is precedent for managing them as UK law enforcement agencies already deal with sources who provide confidential information such as CHIS

[428] U.S. Securities and Exchange Commission, 'Whistleblower Frequently Asked Questions', (2025). [Accessed 23 July 2025].
[429] Hagens Berman, '5 Things Whistleblowers Must Know', [Accessed 31 July 2025].
[430] Serious Fraud Office, *Cooperation Guidance*, (2025).

and assisting offenders. Many serious and complex economic crime cases operate across borders, and therefore managing diplomatic relationships is commonplace.

578. **Further issues** have arisen throughout my conversations. Whilst I do not have answers to these issues, it is important that they are highlighted. The resourcing and administrative implications of introducing effective whistleblower incentivisation schemes are significant. For a scheme to be successful, the administrative function must be adequately equipped to receive and assess large numbers of reports. I understand that the US authorities dedicate specific resource to this aspect of their programmes. Depending on the model used, paying rewards to whistleblowers could prove costly to the State. It is important that the cost is carefully considered against the benefit of receiving information.

579. Eligibility for reward could also prove a tricky area, as policymakers would have to determine whether only those falling within the statutory definition of a whistleblower should be deemed in scope of reward. There are arguments for and against those who are legally obligated to report wrongdoing being eligible, as well as those who have been involved in the criminality themselves or obtained information illegally.

580. It is also worth noting challenges for prosecutors when a whistleblower, who may be eligible for reward, is called to give evidence. Juries may be less likely to trust individuals who, they know, are likely to get a financial reward, concluding that adverse incentives are at play. Instead, law enforcement agencies would be wise to independently corroborate a whistleblower's account during the course of an investigation, to reduce their reliance on testimony and risk of putting an unreliable whistleblower in the witness box. This is of course, easier said than done. It is not unreasonable to expect a defendant to ask the prosecution and the court how an investigation began, and whether they are entitled to know the identity of the whistleblower and the circumstances in which they decide to approach the authorities.

581. Notwithstanding these concerns, it is clear that support for whistleblower incentivisation in the UK is founded on three key arguments, which I outlined in the introduction to this chapter. Firstly, I have heard that UK whistleblowers are currently reporting to US whistleblower programmes. Therefore, UK law enforcement is not receiving valuable information which could assist investigations or uncover criminality. Secondly, whistleblower reports would have the ability to speed up investigations by providing information from the inside. Such information may aid the delivery of swifter justice and the ability of law enforcement to hold culpable individuals and corporates to account.

582. Finally, there is the potential for whistleblower incentivisation to incite real positive cultural changes in corporate behaviour. All companies should be striving to comply with the law and, in cases where they do not, the landscape for a whistleblower is fertile.

Proposals

583. Throughout the course of my review, I have encountered convincing arguments to say that the Government should introduce an economic crime whistleblower incentivisation scheme. It is for this reason that I make the below recommendation.

> **Recommendation 15**
>
> Make legislative provision for the Serious Fraud Office to financially reward whistleblowers. The Government should launch a consultation to inform the design of a suitable scheme.

584. There are several points which I would urge the Government to consult on to design a robust and transparent scheme. Firstly, how the size of the reward is determined. I believe the responsibility of determining the size of a reward best sits with the law enforcement agency rather than a third party such as a judge. It is my view that as the organisation working most closely with the whistleblower, the SFO, will have the truest sense of the value of a whistleblower's information to the investigation.

585. It would be wise for the SFO to conduct an assessment on the value of the information to the case and use this to determine the amount that should be rewarded to the whistleblower, should the prosecution be successful. There should be an agreement in writing between the SFO and the whistleblower to provide mutual understanding of the reward process and payment structure. I believe that open communication with whistleblowers from the outset is most likely to encourage people to come forward.

586. Any scheme where the State is financially rewarding individuals must be transparent, and rewarding agencies should be held accountable for their decisions. Requirements should be placed on those issuing financial rewards to publish an annual report. The report should include figures on the number of whistleblowers who received financial rewards and the value of rewards issued. This process mirrors that of the US, whereby agencies operating whistleblower incentivisation schemes publish an annual report to congress. The Government may wish to learn from this model.

587. I suggest that careful consideration is given to the type of individual that will be deemed eligible under the SFO's whistleblower incentivisation scheme. One such consideration for policymakers would be whether those already under a legal obligation to report wrongdoing could also qualify for a reward. Similarly, there should be clear parameters to determine the type of information that will be accepted under the scheme, and the manner in which the whistleblower obtained that information.

588. Overseas, it is clear that the quality of a whistleblower's legal representation (termed in the US as the 'Whistleblower Bar') is paramount in determining the veracity of referrals

made to law enforcement. Therefore, it is likely that the legal sector would become an integral part of the referral process by ensuring that only the most useful information is put forward to law enforcement.

589. I am aware of calls to establish an Office of the Whistleblower in the UK, and how such a body would add structure to the whistleblowing landscape. Benefits of an Office would include the standardisation of reporting by providing a first port of call for whistleblowers, as well as ensuring protections for whistleblowers and the accountability of rewarding agencies.

590. Whilst noting the benefits that an Office brings, I must also consider the current financial reward landscape. There are already agencies offering rewards in the UK, and it is not within the remit of my Review to redesign the models under which they operate. I believe it would be wise for the Government to learn from the experience of those jurisdictions more advanced in this space when considering the merits of establishing an Office of the Whistleblower alongside incentivisation schemes. Should other agencies follow the SFO and establish schemes, there would be beneficial for the Government to consider a more coordinated approach by establishing a Central Office.

591. Notwithstanding the above, it remains essential that genuine whistleblowers feel safe when coming forward, and that they have a central point of contact should disputes arise. Sufficient guardrails must also be implemented to minimise abuse of any scheme in an attempt to benefit financially.

592. A well-designed whistleblowing regime would complement the SFO's corporate self-reporting policy, shifting the odds towards earlier disclosure. Over time, this should drive more voluntary reports and, in turn, a greater number of Deferred Prosecution Agreements.

593. It is often noted that the rule of law must be present for whistleblower laws to operate with transparency and accountability.[431] Whilst I believe that the democratic resilience of the UK makes the jurisdiction suitable for whistleblower incentivisation, this is an important factor for policymakers to consider should they develop a scheme. For reasons discussed, I make the following recommendations.

[431] Latimer, Pd and Brown, A. J., 'Whistleblower Laws: International Best Practice', *UNSW Law Journal*, vol. 31, no. 3, 2008.

Recommendation 16

Create a new criminal offence for individuals who knowingly make false reports to the law enforcement agencies under a whistleblower incentivisation scheme. The person is not in breach of this offence if he does not know or suspect the report or evidence submitted to be false.

Recommendation 17

Establish a criminal offence for those who harass or intimidate whistleblowers.

Recommendation 18

Establish an independent arbitration panel to review appeals or complaints made by whistleblowers.

12. Investigation

594. Having examined the mechanisms by which fraud is detected and disseminated across the criminal justice system, I now turn to the process of investigation. This chapter seeks to explain how fraud investigations are conducted, how organisational responsibilities are divided, and what barriers exist to their effective execution.

595. It must be recognised at the outset that fraud investigations can differ markedly from investigations into other crimes. Fraud is often online-enabled, cross-jurisdictional, and complex in nature. It may involve multiple victims, shell companies, encrypted communications and international financial flows. As such, it cannot be readily compared with the types of offences typically dealt with by local police forces.

596. Nonetheless, regional and local forces remain a critical part of the national fraud response. While they are tasked with responding to a wide range of crime types, they must be aware of their role within the broader fraud investigation architecture. This chapter sets out that architecture, explains how investigations are initiated and conducted, and evaluates the challenges, both structural and operational, that impede progress.

Enforcement Architecture

597. Responsibility for investigating fraud lies with a range of law enforcement bodies, each with distinct but overlapping roles (see figure 11).

598. **Serious Fraud Office (SFO)**[432] – The SFO investigates and prosecutes the most serious and complex cases of fraud, bribery, and corruption. Operating under the Roskill model, it combines investigative and prosecutorial functions. The SFO typically handles cases involving substantial financial loss, international dimensions, or significant public interest.

599. **National Crime Agency (NCA) and the National Economic Crime Centre (NECC)**[433 434] – The NCA's mission is to protect the public from serious and organised crime, leading the wider law enforcement system against such threats. The NECC, which is housed in the NCA, oversees the operational system response working with Government departments, law enforcement, regulators and the private sector.

600. The NCA, alongside the City of London Police, oversees the National Fraud Squad (NFS), which aims to identify and disrupt serious fraud, domestically and overseas. The

---

432 Serious Fraud Office, '[About us](#)', [Accessed 22 September 2025].
433 National Crime Agency, '[Our mission',](#) [Accessed 22 September 2025].
434 National Crime Agency, '[National Economic Crime Centre](#)', [Accessed 22 September 2025].

NFS consists of a network of approximately 500 specialist investigators across the NCA, City of London Police, and Regional Organised Crime Units.

601. **City of London Police (CoLP)**[435] – As the national lead force for fraud, CoLP plays a central role in policy development, performance monitoring, and victim support.

602. CoLP manages Report Fraud (formally Action Fraud) which is the reporting and analysis service for cybercrime and fraud for England, Wales and Northern Ireland. Report Fraud also offers Victim Services. Additionally, CoLP coordinates the Fraud Protect Coordinators Network to deliver targeted crime prevention messaging to help the public protect themselves from fraud. CoLP also provides training and specialist support to other forces.

603. **National Police Chiefs' Council (NPCC)**[436] – The NPCC is a national coordination body focused on strategic leadership. It brings together chief officers to set priorities and coordinate responses to serious threats such as terrorism, organised crime and national emergencies. Working alongside the College of Policing (CoP), the NPCC develops national standards and approaches for areas including finance, technology, and workforce planning.

604. The NPCC's main decision-making forum is the Chief Constables' Council, which allows for operationally independent chief constables to agree on a national approach to policing.

605. **Regional Organised Crime Units (ROCUs)**[437] – ROCUs were established to tackle cross-border serious and organised crime where local forces were hampered by offenders crossing territorial boundaries. Each ROCU has a dedicated Economic Crime Unit made up of financial investigators and analysts. Increasingly, ROCUs also host Proactive Economic Crime Teams, which are designed to investigate serious fraud, disrupt criminal networks and recover illicit assets.

606. **Local police forces** – The 43 territorial police forces receive the bulk of intelligence packages from the National Fraud Intelligence Bureau (NFIB). They are responsible for investigating the majority of low-level fraud cases and safeguarding victims. Despite limited resources, their role is indispensable.

607. **Insolvency Service** (INSS) – An executive agency of the Department for Business and Trade, the INSS investigates and prosecutes fraud in company and personal insolvencies, including fraudulent trading and director misconduct.[438] It can seek disqualifications, wind up companies in the public interest, recover assets, and bring criminal cases. The INSS

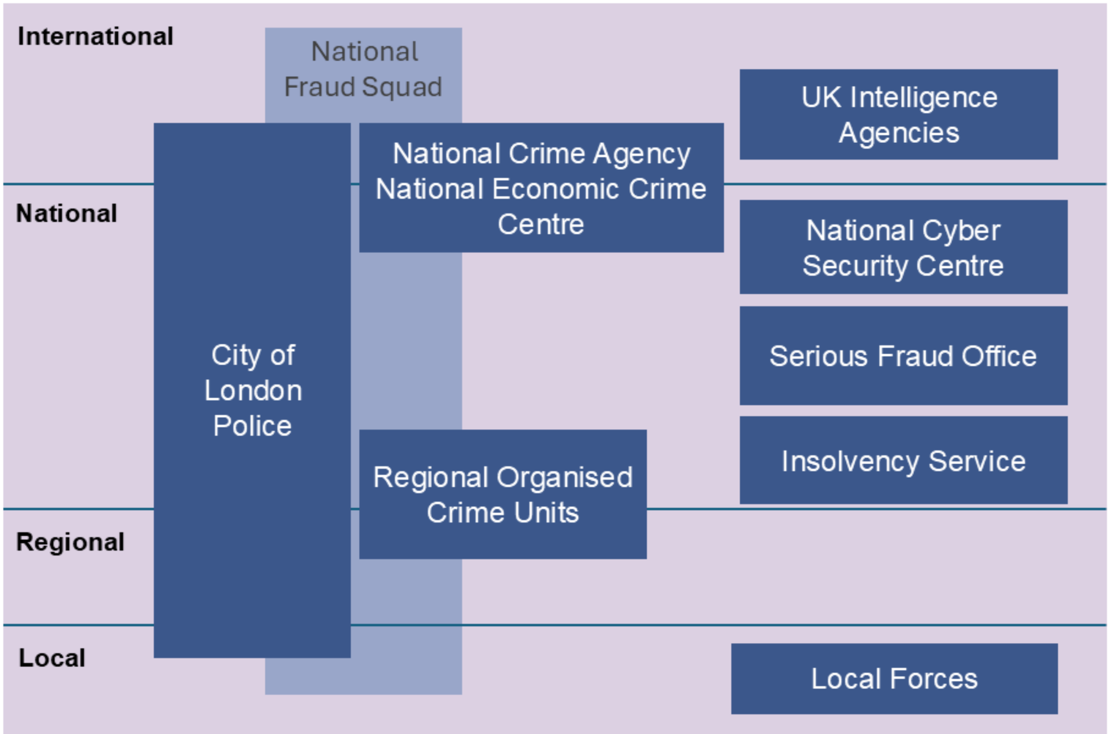
[435] City of London Police, 'National Lead Force', [Accessed 5 September 2025].
[436] National Police Chiefs' Council, 'About Us', [Accessed 5 September 2025].
[437] Regional Organised Crime Unit Network, 'Fraud and Economic Crime', [Accessed 5 September 2025].
[438] The Insolvency Service, 'About Us', [Accessed 5 September 2025].

also acts as the oversight regulator for the insolvency profession, ensuring compliance and maintaining confidence in the regime.

608. **Investigative agencies** – Alongside these policing bodies, it is important to recognise the further agencies which have been granted powers to investigate fraud committed against the State. These include regulatory bodies such as the Competition and Market Authority, National Health Service (NHS) Counter Fraud Authority, Financial Conduct Authority, and HM Revenue and Customs,[439] which can also investigate and/or prosecute fraud. Government agencies such as the Public Sector Fraud Authority can also investigate fraud, recover fraud-related losses and impose non-criminal financial penalties.

609. **UK intelligence community (UKIC)** – The UK intelligence community comprises three primary intelligence services, MI5 (the Security Service), MI6 (the Secret Intelligence Service), and GCHQ (Government Communications Headquarters), along with other Government bodies including Defence Intelligence, the National Cyber Force, the Joint Intelligence Organisation, and the National Security Secretariat. Increasingly, UKIC have played an important role in detecting fraud, particularly those with an overseas dimension.

Fig.11 – Overview of law enforcement agencies with roles in tackling economic crime committed against individuals and businesses



[439] These regulators are discussed in greater detail in chapter 'Data-Sharing'.

610. While each agency has its own purpose, stakeholders repeatedly raised concerns that there remain unclear boundaries between agencies, which allow some fraud cases to fall between institutions. Recent reporting on the collapse of Vashi (Diamond Manufacturers Ltd)[440] highlights how a whistleblower's referral was passed between agencies, with none assuming responsibility, ultimately leaving the matter unresolved before insolvency. This illustrates the operational risk posed by fragmented accountability.

Investigation Process

611. As with all other criminal investigations, fraud investigations are governed by the Criminal Procedure and Investigations Act 1996 (CPIA) and its accompanying Code of Practice.[441] The investigator's duty is to pursue "all reasonable lines of inquiry", whether these point towards or away from a suspect. This principle is central to the fairness of the criminal justice process.

612. However, unlike other offences, fraud investigations do not typically begin with a direct report to a local police station. Given the sheer volume of fraud reports, many of which are low-value or lack actionable intelligence, a triage system has evolved.

613. As detailed in the chapter 'Contemporary Picture', reports are first submitted to Action Fraud—the national reporting centre for fraud and cybercrime.[442] These are assessed by the NFIB, which compiles intelligence packages based on commonalities, leads, and risk indicators. These packages are then disseminated to the appropriate force or agency to consider for potential investigation. This centralised model is designed to prevent local forces from being overwhelmed and to ensure that resources are directed towards cases with the greatest investigative potential.[443]

Law Enforcement Tools

614. Having detailed the investigative process, it is important to explain what tools law enforcement has at its disposal. As detailed in a prior chapter,[444] fraudsters are increasingly exploiting artificial intelligence (AI) to automate procedures, extend their reach, and craft sophisticated deceptions while maintaining online anonymity. In response, law enforcement agencies are beginning to harness this technology in innovative ways.

615. **Disruption** – Police are prioritising upstream interventions, designed to stop fraud before it reaches potential victims. These tactics include removal of fraudulent sites, the

[440] BBC News, 'Jewellery boss in £170m scam told shop staff to pretend to be customers', 1 September 2025.
[441] Ministry of Justice, *Criminal Procedure and Investigations Act 1996 (section 23(1)): Code of Practice*, (2015), point 3.5.
[442] See chapter 'Contemporary Picture'.
[443] See chapter 'Detection and Disruption'.
[444] See chapter 'Fraud Enablers and Connected Criminality'.

deployment of AI chatbots to divert fraudsters from potential victims, and using predictive analytics to identify emerging trends.[445]

616. **Streamlining investigations** – There is a burgeoning industry of private technology firms (such as Nuix and Relativity CloudNine) which are offering law enforcement tools which can assist in streamlining their investigations. Their tools provide investigators with a single unified platform to upload a variety of sources and to utilise AI to classify and contextualise information. This effectively supports investigations by making it easier to identify potentially relevant data and reduce the time spent searching for answers and avoiding false positives associated with keyword-based searches.

617. **Redaction and disclosure** – In a similar vein, and as explored in Part One of this Review, AI technology can dramatically reduce the time officers spend on redaction and disclosure.[446] The Police Digital Service is developing an automated text redaction framework which could see up to 80% time-efficiency savings.[447] Given the tremendous benefits AI can deliver, I reiterate my earlier recommendation that the Government work to ensure sufficient funding to enable for law enforcement agencies to utilise AI in the proactive detection and disruption of fraud.[448]

Recommendation 19

Funding should be prioritised to support the implementation of artificial intelligence by law enforcement agencies in the proactive detection and disruption of fraud.

618. Whilst recognising the transformative potential AI holds for law enforcement, its deployment must be approached with caution. Two key concerns come to mind, beyond those discussed in my first report: overreliance on a single supplier, and erosion of human accountability.

Procurement

619. I reiterate (as discussed in *Disclosure in the Digital Age)* that thought must be given to the procurement process, to ensure that forces are able to access the tools they need in a cost-effective manner.[449]

620. There are several trials across policing, in ROCUs and some local forces, of 'all-purpose' AI products. Whilst they show promise, there is a risk of overreliance on a single supplier.

445 See chapter 'Detection and Disruption'.
446 Home Office, *Disclosure in the Digital Age: Independent Review of Disclosure and Fraud Offences*, (2025), CP 1285.
447 Police Digital Service, 'Police Digital Service redaction tool framework will save police time', press release, 6 March 2024.
448 See chapter 'Detection and Disruption'.
449 Home Office, *Disclosure in the Digital Age: Independent Review of Disclosure and Fraud Offences*, (2025), CP 1285, pp. 131–132

A single supplier may use a proprietary system which is incompatible with others, thereby making migration to alternative systems more cumbersome. This can result in law enforcement agencies being locked into specific systems, subject to cost escalations, the stifling of market innovation and disincentivising continual improvements.

621. With this said, the Government has established its own products. The Public Sector Fraud Authority has built and deployed a Single Network Analytics Platform (SNAP), hosted on the secure cross-Government cloud, to prevent and detect fraud and economic crime in the public and UK's financial services sector.[450]

622. Concerns around procurement are particularly evident when considering the dependence of UK public services on a small number of product suppliers. For example, Palantir has secured contracts with enforcement agencies, the Cabinet Office, the Royal Navy, and the Ministry of Housing, Communities and Local Government.[451] Its increasing presence in policing, through trials in ROCUs and local forces, has sparked discussion, especially around the perceived lack of transparency and the potential for a private firm to access sensitive personal data.[452]

Human Oversight

623. Whilst AI technology is certainly impressive, it is not without errors, perhaps most glaring illustrated by AI hallucinations.[453] These 'hallucinations' are a result of generative AI lacking complete information to respond to prompts and therefore responding with nonsensical or completely fabricated outputs.

624. I mention below two cases within the legal profession in which the hazards of overreliance on AI could lead to the miscarriage of justice. The issue is not the tool itself but rather negligence on the part of practitioners who fail to validate its outputs. When a system consistently produces convincing responses, there is a tendency to step back and trust it uncritically or even to assume the superiority of its judgement.

---

450 Cabinet Office, *Single Network Analytics Platform (SNAP) Privacy Notice*, (2025). [Accessed 5 September 2025].
451 Wilding, M. and Milmo, C., 'UK police working with controversial tech giant Palantir on real-time surveillance network', Liberty Investigates, 16 June 2025.
452 A more detailed discussion on the potential pitfalls of public–private partnerships is detailed in chapter 'Public–Private Partnerships'.
453 AI hallucination – A phenomenon wherein generative AI does not have the complete information it needs to respond to prompts and therefore generates a nonsensical or altogether inaccurate output.

Case Study - *R (Ayinde) v Haringey London Borough Council* [2025][454]

This case concerns two separate claims which were raised in the High Court of Justice concerning the use by lawyers of generative artificial intelligence to produce written legal arguments or witness statements which were not checked.

a. ***Ayinde v London Borough of Haringey*** – A claimant, Mr Ayinde, brought a judicial review against the London Borough of Haringey for failing to provide interim accommodation pending a review of their assessment that he did not have a priority housing need. Subsequently the courts ruled in his favour; however, this judgment relied on cases which did not exist. In total five fictious cases were identified.

b. ***Al-Haroun v Qatar National Bank*** – This concerned a commercial dispute involving a £89.4-million claim. The claimant's legal team submitted 18 fabricated legal authorities, raising serious concerns about the integrity of the legal process.

Whilst the court did not initiate contempt proceedings, the presiding Judge, Dame Victoria Sharp, issued a stern warning noting: "There are serious implications for the administration of justice and public confidence in the justice system if artificial intelligence is misused."

Approaches to Emerging Technologies

625. The approach that should be taken to emerging technology is captured well in the introductory observations of Lord Justice Haddon-Cave and Mr. Justice Swift in the case of *R (Bridges) v South Wales Police* [2019],[455] a case which concerned automated facial recognition technology. The words bear citing in full:

> "3. […] Fifty years ago, the world of forensics and policing was very different. The ability of the police to identify people suspected of criminal offences was largely limited to fingerprint or eyewitness evidence. Advances in modern technology have led to dramatic advances in forensic policing, in particular: the forensic use of deoxyribonucleic acid ('DNA') evidence; closed circuit television ('CCTV') evidence which is ubiquitous; automatic number-plate recognition technology ('ANPR') which is widely used by police forces around the country; and cell-site evidence ('cell-site') which is a feature of many police investigations.

[454] R (Ayinde) v Haringey London Borough Council [2025] EWHC 1383 (Admin).

[455] *R (Bridges) v South Wales Police* [2019] EWHC 2341 (Admin) at [3]-[6].

4. Each advance has naturally given rise to civil liberty concerns. It was never seriously suggested, however, that the police should not be able to make use of those technologies, so long as their use was in accordance with the law. Specific legislative measures were brought into effect in relation to the forensic use of fingerprints, DNA and CCTV (see *e.g.* the Police and Criminal Evidence Act 1984 and the Protection of Freedoms Act 2012). By those measures, and through scrutiny by the Courts of the ways in which such information is gathered, used and retained, the law seeks to strike a sensible balance between the protection of private rights, on the one hand, and the public interest in harnessing new technologies to aid the detection and prevention of crime, on the other."

5. These competing objectives are readily apparent from the leading cases. Lord Steyn's introductory observations in his speech in *R(S) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196, which concerned DNA, emphasised the public benefits in law enforcement agencies using new technology at [1]- [2]:

> '1. It is of paramount importance that the law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science. Such real evidence has the inestimable value of cogency and objectivity. It is in large measure not affected by the subjective defects of other testimony. It enables the guilty to be detected and the innocent to be rapidly eliminated from inquiries. Thus, in the 1990s closed circuit television (CCTV) became a crime prevention strategy extensively adopted in British cities and towns. The images recorded facilitate the detection of crime and prosecution of offenders. Making due allowance for the possibility of threats to civil liberties, this phenomenon has had beneficial effects.
>
> 2. The use of fingerprint evidence in this country dates from as long ago as 1902. In due course other advances of forensic science followed. But the dramatic breakthrough was the use of DNA techniques since the 1980s. The benefits to the criminal justice system are enormous. For example, recent Home Office statistics show that while the annual detection rate of domestic burglary is only 14%, when DNA is successfully recovered from a crime scene this rises to 48%. It is, of course, true that such evidence is capable of being misused and that courts must be ever watchful to eliminate risks of human error creeping in. But as a matter of policy it is a high priority that police forces should expand the use of such evidence where possible and practicable.'

6. The counterpoint is readily apparent from Lord Reed's observations in *R(T) v Chief Constable of Greater Manchester* [2015] AC 49 at [88]:

> 'The United Kingdom has never had a secret police or internal intelligence agency comparable to those that have existed in some other European countries, the East German Stasi being a well-known example. There has however been growing concern in recent times about surveillance and the collection and use of personal data by the state. … But such concern on this side of the Channel might be said to have arisen later, and to be less acutely felt, than in many other European countries, where for reasons of history there has been a more vigilant attitude towards state surveillance. That concern and vigilance are reflected in the jurisprudence of the European Court of Human Rights in relation to the collection, storage and use by the state of personal data. The protection offered by the common law in this area has, by comparison, been of a limited nature.'"

Transparency and Accountability

626. As agencies adopt new technologies, efforts must be made to guard against overreliance that undermines human accountability. Transparency and oversight are essential, especially in the deployment of AI. Law enforcement agencies must be able to 'open the black box', to interrogate and explain how algorithms reach their conclusions, ensuring clarity, accountability and lawful application. The need for transparency has been recognised by the *Covenant for Using Artificial Intelligence (AI) in Policing*,[456] which sets out sensible, high-level principles to abide by when adopting AI, noting that the UK has a core tradition of policing by consent, and the principles will help maintain this in an AI context. Among these measures, the police must take to ensure that AI deployment is lawful, transparent, and founded on robust data.

627. Means by which the public can gain a greater understanding of what tools are being utilised by the police should be explored. This could include a voluntary data collection exercise or more formal use of Secretary of State powers under S44 Police Act 1996[457] ('Provision of information by Chief Officers of Police') to require every force to disclose information. Other routes to encourage transparency include requesting forces publish this information on their websites, alongside named accountable officers for each AI deployment.

Systemic Barriers

456 National Police Chiefs' Council, *Covenant for Using Artificial Intelligence (AI) in Policing*, (2023).
457 Police Act 1996, s.44.

628. Having outlined the investigative architecture and the array of tools available to investigators, I turn to examine the systemic issues which constrain law enforcement. This ranges from the chronic under-prioritisation of fraud, inconsistent monitoring, and shortfalls in specialist staffing and appropriate training.

629. Ministerial focus has historically centred on high-harm crime types such as violence against women and girls, knife crime, and county lines.[458] While certainly important, such policies have allowed fraud offending to grow unchecked. Recently, however, successive governments are now beginning to recognise fraud as a national security threat.[459] [460] Further barriers include:

   a. **Competing operational demands** – These mean that forces are often drained by life-threatening and time-sensitive incidents. However, fraud is not a victimless crime. It is frequently interlinked with other offences, and its victims, often dispersed and reluctant to report due to shame, are no less deserving of protection.

   b. **Investigative complexity** – Fraud cases demand specialist skills, digital forensics, financial analysis, legal expertise—that are not readily available in many forces. This creates a structural disincentive to pursue such cases

   c. **Performance metrics** – Fraud statistics are not routinely included in local or regional performance data, despite being investigated at those levels.[461] Reduced visibility and accountability regarding local force prioritisation of fraud cases inhibit the ability to diagnose which parts of the local law enforcement response are working well and which forces are sidelining fraud investigations.

630. Beyond prioritisation, fraud investigations are constrained by resource limitations and fragmented governance structures. These challenges manifest differently at local and regional levels

   a. Local forces:

      i. **Strategic under-recognition** – Many local forces fail to appreciate the strategic importance of fraud or its connection to other crime types. There is also limited awareness of the upstream disruption work undertaken by the NFS.

---

458 Home Office, 'Government to launch new coalition to tackle knife crime', news story, 9 September 2024.
459 HM Government, *Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy*, (2021), CP 403, page 82.
460 HM Government, *Integrated Review Refresh 2023: Responding to a more contested and volatile world*, (2023), CP 811, paragraph 15.
461 House of Commons Justice Committee, *Fraud and the Justice System: Government Response to the Committee's Fourth Report of Session 2022–2023*, (2023), HC 1020, pp. 7–8.

ii. **Lack of specialist teams** – Most local forces rely on non-specialist investigators, who often lack the expertise required for complex fraud cases. This mismatch between offence volume and investigative capacity is a recurring concern.

b. Regional forces:

i. **Staff shortages** – High turnover and short-term contracts mean that many officers do not see a fraud case through to conclusion. The public sector's inability to match private sector salaries has led to a talent drain. The NECC's Fraud Targeting Cell has also faced recruitment and resourcing difficulties, resulting in fewer cases being passed to ROCUs and in inconsistent tasking.

ii. **Limited career progression** – The absence of clear promotion pathways and specialist development opportunities exacerbates retention issues.

iii. **Fragmented recruitment** – Investigators are often rushed into operational roles without adequate preparation. It can take one to two years before they are fully trained, and with the current delays in the criminal justice system, this may result in an investigator not being able to see a single fraud case from initiation through to completion.

iv. **Funding disparities** – Equal funding across ROCUs fails to reflect regional variations in fraud threat, geographical coverage or existing capabilities. Some ROCUs require specialist posts and higher salary bands, which the current model does not accommodate.

Training

631. Technical capability is hampered by digital skill shortages, particularly in areas such as digital forensics.[462] Assessments highlight widespread challenges in recruiting specialists, prioritising training and standardising provision. Notably, there is no mandatory training in fraud investigation.[463]

632. The structure of police training presents further obstacles. The two principal bodies which oversee fraud-related training are CoLP and CoP.

633. CoLP offers optional training to all officers through its Economic and Cyber Crime Academy. The academy offers accredited training courses to cater to specialist and non-specialist investigators. They are currently developing a new optional introductory course

[462] National Police Chiefs' Council, *Digital Forensic Science Strategy*, (2020).
[463] HM Inspectorate of Constabulary and Fire & Rescue Services, *An inspection into how well the police and other agencies use digital forensics in their investigations*, (2022).

known as ‘Every Officer is a Fraud and Cyber Officer’, aimed at ensuring that fraud, cyber and economic crime are embedded within all officers’ training, as this area of criminality is widespread and links to several other crime types.

634. CoP, instead, focuses on general training, offering Professionalising Investigations Programme (PIP) One and Two, with courses in core investigative skills, including digital investigations. It also provides Operation Modify, an online package aimed at improving digital intelligence capabilities. Their website includes Authorised Professional Practice on fraud, which links a wide range of practical guidance to support general and frontline investigators who are assigned a fraud case. A single document providing a short, accessible and practical overview of fraud investigations should be developed.

635. Feedback from law enforcement officers’ highlights three key concerns:

a. **Lack of clarity** – Despite efforts to align content, there remains confusion over the distinction between CoLP and CoP training, leading to duplication and inefficiency.

b. **Inconsistent monitoring** – Data collection on training completion and skill acquisition varies widely. Forces must determine which metrics to capture, e.g. PIP accreditation levels, course types, turnover rates, and build systems accordingly.

c. **Absence of formal assessment** – CoLP’s Economic and Cyber Crime Academy courses lack formal evaluation mechanisms since impact assessments and feedback loops are not routinely conducted.

636. There is a clear role for CoP, as the independent standards body, to assess and accredit CoLP’s specialist courses. CoLP, as the national lead force for fraud, should retain responsibility for design and delivery.

637. CoLP engaged with the Home Office and HM Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) to ensure fraud is included in the annual Police Efficiency, Effectiveness and Legitimacy (PEEL) assessments. This is a welcome step towards rigorous and consistent evaluation.

638. As a specific example, stakeholders consistently highlighted the acute challenge of recruiting and retaining financial investigators. While not required in every fraud case, their expertise in tracing assets and in Proceeds of Crime Act 2002 (POCA) powers is critical. Demand for these skills far exceeds supply, with law enforcement competing against lucrative private sector roles in banking, insurance and technology. In 2023, a freedom of information request for HMICFRS revealed that in one Metropolitan Police operational hub, only eight financial investigators were in post against an establishment

of 50, leaving some units operating at less than 20% of required strength.[464] CoLP's National Economic Crime Workforce Strategy[465] also acknowledges persistent retention challenges and calls for structured career pathways and incentives to stem losses.

639. The barriers outlined, from strategic under-prioritisation to fragmented training and governance, require a coherent response. Law enforcement agencies must be well trained and engage officers who are motivated to take on fraud cases.

Conclusion

640. With fraud constituting a significant proportion of domestic crime, the investigation of such cases is not a peripheral task but should be a core criminal justice mission; however, only 1% of policing resources are applied to this crucial task.[466]

641. The operational reality is a painful story of a system carrying significant deficiencies, fragmented governance, chronic under-prioritisation, and acute shortages of specialist personnel. Recruitment and retention of skilled investigators, particularly financial investigators, remain critical vulnerabilities. Without a strong police force that is not only sufficient in number but equipped with the requisite training and tools, the State cannot realistically hope to increase criminal justice outcomes for fraud.

642. Investment in technology, including AI, offers transformative potential. However, such tools must complement, not supplant, human judgement. Training must embed accountability and guard against overreliance on automated systems. Procurement must avoid monopolistic dependencies and ensure interoperability.

643. Above all, investigative roles, particularly those focusing on economic crime and fraud, must be made attractive. Clear career pathways, competitive remuneration and professional recognition are essential to stem the talent drain to the private sector.

644. The Home Office is exploring opportunities to strengthen and unify the fraud law enforcement approach from local through to national with clearer responsibilities and more effective tasking.

---

[464] HM Inspectorate of Constabulary and Fire & Rescue Services, 'HMICFRS - 300 staff vacancies in Specialist Crime Command', FOI request no. 01.FOI.23.030532, (2023).
[465] City of London Police, *National Policing Strategy for Fraud, Economic and Cyber Crime 2023 – 2028*, (2023), page 18.
[466] Home Office, *Fraud Strategy: stopping scams and protecting the public*, (2023), CP 839.

13. Powers

645. In the investigation of fraud offences, officers face a distinct and increasingly complex set of evidential challenges. Unlike traditional crimes, fraud is predominantly committed online, leaving behind a digital trail that must be carefully traced and interpreted. Investigators are routinely required to navigate encrypted communications, anonymised transactions, and remote data storage—often across multiple jurisdictions.

646. Technological advances, particularly in encryption and decentralised finance, have created formidable barriers to law enforcement. Accessing critical evidence stored on electronic devices or remote servers is frequently obstructed by sophisticated security protocols.

647. The rise of cryptocurrencies has compounded these difficulties. Their pseudonymous and decentralised nature allows offenders to bypass regulated financial institutions, making it harder to trace illicit funds. Investigators must engage in complex blockchain analysis to identify suspect wallets and follow the flow of transactions. This task is further complicated by the use of obfuscation tools such as 'tumblers' or 'mixers', which pool and redistribute coins across multiple addresses, rendering forensic tracing exceptionally difficult.

648. In short, technological innovation has outpaced the investigatory powers available to police, making the identification and seizure of criminal material, and the proceeds of crime, an increasingly arduous endeavour.

649. Given these advances in technology, considerable effort has been spent in modernising the legislative framework, yet still the core statutory powers to investigate fraud pre-date the advent of the technological innovations discussed. I outline below key pieces of legislation granting power to law enforcement to conduct searches and seize material relevant to the investigation, compel disclosure, intercept communications, impose freezing orders and repatriate assets.

Current Legislative Framework

Powers of Entry, Search and Seizure

650. The Police and Criminal Evidence Act 1984 (PACE) is the foundational statute governing police powers in England and Wales. It provides the framework for police to be able to enter and search a suspect's premises and seize property in relation to an indictable offence, including fraud. Search warrants in connection with fraud investigations can be obtained under multiple other statutes, including section 387 of the Proceeds of Crime Act 2002 (POCA), section 2(4) of the Criminal Justice Act 1987 (CJA 1987), and section 176 of the Financial Services and Markets Act 2000.

651. Under the Criminal Justice and Police Act 2001, a person may seize property which contains relevant material in order to sift the property off-site if it is not practicable to identify or segregate the relevant material on premises. This power is frequently exercised where a device is suspected to contain legally privileged material which cannot be searched for or seized.

652. POCA is an example of a statute which provides a suite of investigatory powers (under Part 8 of POCA) alongside distinct enforcement regimes. For example, Part 2 of POCA governs the confiscation regime, which is a post-conviction process aimed at depriving criminals of the financial benefits of their crimes. It contains powers to restrain (section 41) and seize (section 47C) property with a view to satisfying any confiscation order that has been or may be made against a defendant.

653. In contrast, Part 5 of POCA enables law enforcement to engage with the civil recovery of property through unlawful conduct, even when no criminal conviction has been secured. These powers under POCA were further enhanced by the Economic Crime and Corporate Transparency Act 2023 (ECCTA), which introduced specific provisions to deal with cryptocurrency. These include allowing law enforcement to:

a. Search, seize, and detain crypto-assets suspected of being linked to crime.

b. Apply for freezing orders to prevent the movement of crypto-assets during investigations.

c. Forfeit crypto-assets permanently if they are proven to be proceeds of crime.

d. Use conversion orders to convert crypto-assets into *fiat* currency for lawful handling.

Powers of Production

654. There are a number of statutory powers which empower an investigator to require the production of, or access to, material and documents, which include electronic devices or electronic data. Some of these powers may be exercised while executing a warrant, or instead of obtaining a search warrant:

a. Under section 19(4) of PACE, a constable who is lawfully on premises may require the production of electronic data if they have reasonable grounds for believing (1) it has been obtained in consequence of the commission of an offence or is evidence in relation to any offence; and (2) it is necessary to require its production in order to prevent it being concealed, lost, altered or destroyed.

b. Under section 20(1) of PACE, certain powers of seizure which apply to constables are construed as including a power to require electronic data to be produced in a visible and legible form.

c. There are powers to apply to a court to obtain a production order under various statutes. This includes Schedule 1 to PACE and section 345 of POCA. A production order typically requires a specified person to produce material within a specified period, give access to the material or state the material's location.

d. Some powers of production do not require recourse to a court. The Director of the Serious Fraud Office may issue a notice under section 2(3) of CJA 1987 requiring the production of documents.

e. Major investigative agencies can apply for an overseas production order under the Crime (Overseas Production Orders) Act 2019 against a person who has possession or control of electronic data, which requires the person to produce or provide access to the data. Such a power can only be applied for where a designated international cooperation arrangement exists and permits such orders. At present, an agreement is only in place with the United States of America (US).

Powers to Request Legal Assistance from Other States

655. Generally speaking, investigative powers cannot operate extraterritorially. For example, the police could not compel a person abroad to produce electronic data, or travel to execute a search warrant on a premises outside of the United Kingdom (UK). Overseas evidence is often relevant to a UK criminal investigation. In such instances, UK law enforcement agencies may request assistance from other states in order to obtain evidence in criminal investigations. Overseas electronic data may be requested pursuant to a letter of request sent by the UK to a state where the data is stored. This avenue requires the requested state to consider and grant the request.

656. The UK and other states have entered into international agreements concerning mutual legal assistance. For example, on 6 January 1994 the UK and the US signed a bilateral treaty on mutual legal assistance pursuant to which their respective law enforcement authorities could request assistance in investigating criminal matters, including the provision of documents, records and evidence.

657. I discuss international cooperation in further detail in the next chapter.

Powers to Compel Access to Devices and Data

658. Under section 49 of the Regulation of Investigatory Powers Act 2000 (RIPA), a person with 'appropriate permission', who falls within Schedule 2 of RIPA, has the power to impose a disclosure requirement on a person believed to have possession of a 'key' to 'protected information' where the conditions in section 49(2) of RIPA are met. The section applies where protected information has come into the possession of any person by means of the exercise of a statutory power to seize, detain, inspect or search, or is likely to do so.

659. Schedule 2 provides the definition of appropriate permission:

a. Paragraph 1(1) of Schedule 2 states a person has the appropriate permission in relation to any protected information if, and only if, written permission for the giving of section 49 notices in relation to that information has been granted by a Circuit judge (or a District Judge (magistrates' courts) following amendment by paragraph 12 of Schedule 4 to the Courts Act 2003).

b. Paragraph 2 deals with unintelligible information which is or is likely to be obtained under a statutory power exercised in accordance with *inter alia* a warrant issued by a person holding judicial office (including a justice of the peace), such as a search warrant under POCA. A warrant may empower a person to serve a notice requiring disclosure if the warrant gave explicit permission for the notice to be given. This means that a magistrate may grant permission to impose a disclosure requirement at the point of granting a warrant. The warrant must therefore contain explicit permission for giving section 49 notices in relation to protected information to be obtained under the warrant.

660. Section 56(1) of RIPA defines the following terms:

a. 'Key', in relation to any electronic data, means any key, code, password, algorithm or other data the use of which (with or without other keys) allows access to the electronic data or facilitates the putting of the data into an intelligible form.

b. 'Protected information' means any electronic data which, without the key to the data, cannot, or cannot readily, be accessed or put into intelligible form.

661. Section 53(1) provides that a person to whom a section 49 RIPA notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the required disclosure. Section 53(5A) provides that the maximum penalty in a national security case or a child indecency case is five years and, in any other case, two years.

662. Section 53(2)-(3) imposes an evidential presumption and reverse burden: if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 49 notice, that person <u>shall be taken</u> to have continued to be in possession of that key at all subsequent times (the evidential presumption), <u>unless it is shown</u> that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it (the reverse burden). The reverse burden is an evidential one: a person shall be taken to have shown that he was not in possession of a key to protected information at a particular time if sufficient evidence of that fact is adduced to raise an issue with respect to it and the contrary is not proved beyond a reasonable doubt.

663. A requirement of disclosure of knowledge of the means of access to protected data under compulsion of law will not engage the privilege against self-incrimination unless the electronic data itself, which exists independently of the person's will and to which the privilege does not apply, contains incriminating material (*R v S* [2008] EWCA Crim 2177, [2009] 1 WLR 1489 at [24]).

Powers to Intercept Communications and Interfere With Equipment and Property

664. The Investigatory Powers Act 2016 (IPA) governs the interception of communication and enables law enforcement to collect bulk data, requires internet service providers to retain records of websites visited by users for 12 months, and authorises hacking under strict warrants. Warrants are to be issued by the Secretary of State and must be approved by a judicial commissioner. The grounds for such a warrant include concerns over national security, preventing or detecting serious crime (which includes fraud), and safeguarding the economic wellbeing of the UK (in certain circumstances).

665. The interference with electronic devices is principally governed by two regimes. What is called 'equipment interference' is governed by IPA, whereas 'property interference' is governed by Part III of the Police Act 1997 and the Intelligence Services Act 1994.

666. The terms 'equipment' and 'property' can both be read as covering electronic devices for present purposes. Whether interference falls into either category depends on the purpose for which the interference occurs rather than the material that is the subject of the interference. Generally speaking, where the main purpose of the interference is to obtain electronic data, the conduct will constitute equipment interference, otherwise the conduct will constitute property interference. For example, property interference will be engaged where the purpose of interference is to disable or neutralise an electronic device.

Gaps in Investigatory Powers for Fraud

Shifting Roles

667. Plainly, each law enforcement agency requires the right powers to tackle the types of fraud for which they are responsible for pursuing, forms range from simple email-based deceptions to multi-million-pound corporate investment frauds. However, I have heard concerns that some large fraud cases, which do not qualify for the Serious Fraud Office (SFO), are not being swiftly gripped by the system but instead passed around until an agency agrees to own them.

668. It is into this context that the Insolvency Service (INSS) has announced a significant change in its enforcement strategy, recognising the gap in the law enforcement puzzle and committing to a more assertive role in tackling corporate fraud. This ambition, however, must be matched by the powers and resources necessary to deliver it.

669. The INSS's new *Investigations and enforcement strategy 2026 to 2031*[467] signals a decisive shift from a primarily reactive insolvency-focused model to a proactive economic crime mandate. The Service intends to target complex corporate fraud cases that fall below the SFO threshold but pose systemic risks to market integrity and creditor confidence.

670. These include phoenix companies,[468] large-scale director misconduct, and fraud exploiting corporate structures to conceal assets or facilitate money laundering. The strategy emphasises intelligence-led interventions, leveraging enhanced data flows from Companies House reforms under the Economic Crime and Corporate Transparency Act 2023. The INSS aims to act earlier in the fraud lifecycle, disrupting schemes before insolvency crystallises.

671. Unlike the SFO, the INSS operates without core statutory powers that other enforcement bodies, undertaking proactive enforcement, take for granted. Its investigators cannot compel attendance at interviews under caution, nor can they execute search warrants or effect arrests. These limitations mean investigations depend on voluntary cooperation or ad hoc police assistance, often secured through personal relationships, which presents challenges.

672. Current powers under PACE are confined to obtaining special procedure material under section 9 and Schedule 1, and even then, warrants must be executed by a constable. This challenge is not a new one. The Law Commission recommended in 2020 that the INSS be granted authority to obtain and execute search warrants under section 8 PACE, yet this reform remains unrealised.[469] The absence of arrest powers compounds delay: suspects decline voluntary interviews or exploit the lack of compulsion to postpone, repeatedly. In May 2025, the Ministry of Justice published an update regarding the implementation of the Commission's recommendations noting that "significant changes" were made, and search warrants legislation will continue to be reviewed "to ensure the system works effectively".[470]

673. I therefore recommend that the Government prioritise this proposal. These reforms would align the INSS with best practice and deliver a credible deterrent against corporate fraud, complementing the work already undertaken by the SFO. Implementation will require operational training, oversight mechanisms, and safeguards against misuse, alongside consultation to balance enforcement with legitimate business concerns.

---

467 The Insolvency Service, *Investigations and enforcement strategy 2026 to 2031*, (2025).
468 Phoenix company – A business that is deliberately wound up or liquidated to shed debts and liabilities, only for its directors to immediately start a new company with substantially the same assets, operations or identity, often to continue trading while avoiding obligations to creditors.
469 Law Commission, *Search warrants*, (2020), HC 852, Law Com No 396, recommendation 8, paras 3.42–3.45.
470 Ministry of Justice, *Report on the implementation of Law Commission recommendations*, (2025), HC 850, paragraphs 69-72.

Recommendation 20

The Law Commission recommendation 8, from its report *Search Warrants* (2020), should be implemented.

Namely that the Insolvency Service be empowered to execute search warrants obtained under the Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002, without the need to accompany a constable. This would extend to exercising the powers of entry as well as search.

That sections 19 to 22 of the Police and Criminal Evidence Act 1984 be extended to the Insolvency Service, with necessary modifications.

<u>Phoenixing</u>

674. This Review also heard proposals for a summary-only phoenixing offence, to be considered in light of the Economic Crime and Corporate Transparency Act 2023, and repositioning of Companies House into an active regulator with powers to verify director identities, query filings, and share intelligence with law enforcement. The Company House reforms will generate richer data on repeat directorships and suspicious corporate patterns, creating an opportunity to identify serial phoenix behaviour earlier and support proportionate enforcement.

675. Reflecting on my experience as a practitioner, I encountered cases where directors closed a company to wipe out its debts, only to launch a new enterprise almost immediately, using nominee directors and senior managers. This successor business often mirrored the original, reusing assets and continuing the same operations, allowing those behind it to trade on while sidestepping their obligations to creditors.

676. While this Review recognises the potential merit in creating a bespoke offence to address such conduct, the evidence presently available does not justify recommending one at this stage. Any proposal would require further consultation to ensure consistency with emerging intelligence-sharing frameworks and to guard against unintended consequences for legitimate enterprise.

677. I also note that the Law Commission made similar recommendations in respect of the National Health Service (NHS) Counter Fraud Authority. This body investigates fraud committed within the NHS and is therefore properly regarded as fraud against the State, outside the scope of this Review. Nonetheless, there is merit in the Government revisiting

those recommendations and considering whether the Authority has the powers necessary to discharge its mandate effectively.[471]

Lack of Extraterritorial Reach

678. One issue on which I heard concern was the lack of extraterritorial reach of powers to compel the production of, and seize, overseas material. Again, this is a limitation in investigatory powers I have seen in practice. There are a host of production powers on the statute book, several of which can be sought in fraud investigations. I heard particular concern from the SFO over the limited territorial reach of their powers under section 2(3) of CJA 1987. It is this power on which I will focus, given that it is concerned exclusively with the investigation into serious or complex fraud.

679. The question is this: what happens if the SFO wishes to compel the production of material held overseas? The SFO has four options if it wishes to obtain evidence overseas:

a. First, the SFO may serve a section 2(3) CJA 1987 notice in this jurisdiction on a UK individual or company or foreign individual or company with an actual presence in the UK. This is the result of the Supreme Court's decision in *SFO v KBR* [2021] UKSC 2, which I will discuss below.

b. Second, the SFO may seek voluntary disclosure from the individual or company. Where criminality is suspected, there will be little incentive to comply.

c. Third, the SFO may avail itself of mutual legal assistance channels by issuing a letter of request to the foreign state to assist in obtaining the relevant documents. This depends on whether material is held in a jurisdiction in which a bilateral or multilateral treaty is in force. Mutual legal assistance is also a slow and cumbersome procedure.

d. Fourth, the SFO may apply for an overseas production order under the Crime (Overseas Production Orders) Act 2019. However, only one international cooperation agreement exists, which is with the US. An overseas production order can only, therefore, be used to compel a foreign individual or company which operates, or is based, in the US to produce specified electronic data of which it has possession or control.

680. Given the shortcomings of the second, third and fourth options with obtaining overseas material, the extraterritorial reach of section 2(3) CJA 1987 is clearly an important matter. It was the question which occupied the Administrative Court ([2018] EWHC 2368 (Admin)) and Supreme Court ([2021] UKSC 2) in the *KBR* litigation. As put by Gross LJ, giving the judgment of the Administrative Court in KBR at [69]:

[471] Law Commission, *Search warrants*, (2020), HC 852, Law Com No 396., recommendation 7, paras 3.15–3.21.

> "The context here concerns the investigation and prosecution of top-end fraud. There is, accordingly, an extremely strong public interest in the extraterritorial ambit of s.2(3), which is anything but a private matter. That public interest extends to the UK's international obligations under instruments such as the *OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions* (2011)."

681. The Administrative Court ([2018] EWHC 2368 (Admin)) held that Section 2(3) extends extraterritorially to foreign companies in respect of documents held outside the jurisdiction when there is a sufficient connection between the company and the jurisdiction. The reasoning was as follows:

   a. Section 2(3) must have some element of extraterritorial application. It would be unfortunate if an otherwise lawful notice could be resisted and a serious fraud investigation forestalled by transferring documents abroad.

   b. The question was whether the extraterritorial application extends to foreign companies. There would be a very real risk that the legislative purpose of section 2(3), the investigation and prosecution of complex fraud, would be frustrated if the SFO was precluded from seeking documents held abroad from any foreign company.

   c. The right answer to the jurisdictional ambit of section 2(3) was a nuanced answer. Section 2(3) extended extraterritorially to foreign companies in respect of documents held outside the jurisdiction when there was a sufficient connection between the company and the jurisdiction.

682. The Supreme Court ([2021] UKSC 2) overturned the decision of the Administrative Court with the following reasoning:

   a. Section 2(3) included no express provision to rebut the presumption against the statute having extraterritorial effect and there was no clear indication either for or against extraterritorial effect in other provisions of CJA 1987.

   b. The legislative history to CJA 1987 provided an indication that Parliament intended that evidence should be secured from abroad by international cooperation. Successive provisions also provided support for the view that Parliament did not intend those later powers, operating through reciprocal cooperation with foreign authorities, and the statutory protections and safeguards to which they are subject, to sit alongside a unilateral power in CJA 1987 s.2(3) of the breadth contended for by the SFO.

   c. It was inherently improbable that Parliament should have refined this machinery as it did, while intending to leave in place a parallel system for obtaining evidence from abroad which could operate on the unilateral demand of the SFO, without any recourse to the courts or authorities of the State where the evidence was located, and without the protection of any of the safeguards put in place under the scheme of mutual legal assistance.

683. The SFO explained that the effect of the Supreme Court's ruling does create practical barriers to obtaining overseas evidence. Three examples were given to illustrate the challenges with securing overseas evidence:

a. Where a director of a UK company has committed fraud but then left the jurisdiction, a notice cannot be served overseas.

b. A foreign corporate without a UK presence but with a UK connection cannot be served with a notice. Where a UK subsidiary uses a server owned by an overseas parent company, emails and files can fall outside the reach of a section 2(3) notice.

c. Similarly, the UK branch of an international banking group may be unable to produce documents concerning a UK customer as the records are controlled by overseas headquarters. Mutual legal assistance may not be possible depending on the jurisdiction concerned.

684. In considering reform, several important but competing public interests are at play. The first, identified by Gross LJ, is the public interest in ensuring that the SFO has the tools necessary to investigate and prosecute top-end fraud. The second is the public interest in ensuring that the UK respects international rules of jurisdiction and comity and avoids the exorbitant exercise of jurisdiction. The third is the public interest in protecting the personal and property rights of citizens.

685. I am alert to the principles of international comity. The UK cannot adopt a brightline rule that it can compel foreign entities to comply with its laws and provide overseas material on pain of punishment. Nor would statutory amendment ameliorate all of the SFO international investigation short fallings Mutual legal assistance will always be necessary to obtain certain categories of overseas material. However, mutual legal assistance is not a panacea given its shortcomings. The framing of the CJA is antiquated and merits revisiting. The landscape of fraud has significantly evolved in the decades since the Act was first introduced. I also consider that a revised power may complement and assist in securing mutual legal assistance and could provide the coercive tools needed to compel individuals overseas to return to the UK to cooperate with an investigation.

686. I am therefore of the view that section 2(3) does not presently strike the right balance between the various public interests which it engages. For my part, I see sense in extending the SFO's ability to compel the production of overseas material in each of the cases it identified. That said, I recognise that any amendment engages significant and complex questions, including appropriate procedural safeguards, navigating potential conflicts of laws, and ensuring respect for international comity.

687. For example, the answer for extraterritorial expansion might be a nuanced one, requiring a sufficient connection to the UK jurisdiction, as recognised by Gross LJ, although later dismissed by the Supreme Court as impermissible judicial lawmaking.

688. I note ECCTA has provided an example on how this could be framed. ECCTA introduced a new 'failure-to-prevent' fraud offence, which has explicit extraterritorial reach applying where there is a 'UK nexus'.

689. This nexus is met if at least one element of the fraud occurs in the UK, or the intended gain or loss must arise in the UK. The offence does not apply to UK organisations whose overseas employees or subsidiary undertakings commit fraud abroad with no UK nexus. As with ECCTA, a reformed CJA 1987 should include guidance which makes clear what qualifies as 'sufficient UK connection', to prevent jurisdictional overreach.

690. As for actual extraterritorial service of a notice by serving it outside the jurisdiction, this raises particularly sensitive issues. Currently, only overseas production orders, underpinned by a ratified bilateral treaty, permit extraterritorial service of a coercive compulsion notice. It seems to me that there is nonetheless a powerful argument to permit extraterritorial service of a notice on a UK person who is a director of a UK company who is overseas.

691. In terms of defining a UK person, one option would be to adopt the definition in section 21 of the Sanctions and Anti-Money Laundering Act 2018, namely:

a. A UK national, that being:

    i. A British citizen, a British Overseas Territories citizen, a British National (Overseas) or a British Overseas citizen.

    ii. A person who under the British Nationality Act 1981 is a British subject.

    iii. A British protected person within the meaning of that Act.

b. A body incorporated or constituted under the law of any part of the UK.

692. Ultimately, I agree with the Supreme Court that such a reform will require legislative footing and should be subject to robust parliamentary debate. This is why I am unable to reach a firm conclusion on reform. Rather, I recommend that the extraterritorial ambit of section 2(3) of CJA 1987 be reviewed.

Recommendation 21

The extraterritorial ambit of section 2(3) of the Criminal Justice Act 1987 should be reviewed at with a view in particular to expanding jurisdiction to enable the Serious Fraud office to serve a notice on:

a. A United Kingdom (UK) person who is a director of a UK company and who is overseas.

b. A foreign corporate without a UK presence but a sufficient UK connection.

Compelling Access to Devices and Data

693. I heard concerns about the power to impose a disclosure requirement on a person believed to have possession of a key to protected information under RIPA. These concerns were as follows.

694. **Required level of judicial officeholder** – A key concern I have heard from law enforcement agencies regards the lengthy process involved in securing approval for section 49 notices under RIPA. I was told that Schedule 2 specifies that a section 49 notice requires written permission from a Circuit judge in England and Wales to compel suspects to provide a key to bypass encryption. This constrains authorisation for section 49 notices within the mid-level judiciary.

695. I have heard concerns that this structure is unnecessarily cumbersome and can cause significant delays. A delay in on-site access to a device prevents agencies from triaging digital devices there and then, if a password is not forthcoming, the device often has to be seized, with its storage thereafter being subject to the Criminal Procedure and Investigations Act 1996 (CPIA) and disclosure duties, extending the investigation further.

696. I observe that, in fact, paragraph 1(1)(a) of Schedule 2 to RIPA allows appropriate permission to be granted by a Circuit judge or a District Judge (magistrates' courts), as inserted by paragraph 12 of Schedule 4 to the Courts Act 2003. There is, however, a note on the professional legal database Westlaw which suggests doubtful commencement:

> "Paragraph 1(1)(a) is amended so as to give District Judges (magistrates' courts) parallel jurisdiction with Circuit Judges. There is some room for doubt as to the commencement status of this amendment, which is made by paragraph 12 of Schedule 4 to the Courts Act 2003 (introduced by section 65(2)). Section 65 was commenced as of 1 April 2005 by article 3(u) of the Courts Act 2003 (Commencement No. 10) Order 2005, which says nothing about Schedule 4: there is evidence either way within the Order as to whether the omission is significant or effective. Government publications appear inconsistent on the point, some suggesting that

paragraph 17 is in force and some suggesting that it is not. There is an argument that the legislative intent of article 3(u) in commencing the whole of section 65 should be given effect by implying the commencement of Schedule 4, and the failure to mention Schedule 4 separately should be regarded as a drafting inconsistency of the kind that the courts would be prepared to rectify under the rule in *Inco Europe*."

697. My view is that paragraph 1(1)(a) of Schedule 2 to RIPA should be read as allowing appropriate permission to be granted by a District Judge (magistrates' courts).

698. Relatedly, I have considered whether appropriate permission should also be able to be granted by a magistrate or 'lay justice', as defined in section 9 of the Courts Act 2003 as a justice of the peace who is not a District Judge (magistrates' courts). Both lay justices and District Judges (magistrates' courts) can authorise search warrants under PACE. Magistrates undertake mandatory training and are supported in court by a qualified legal adviser. I therefore regard magistrates as more than capable of dealing with applications under section 49 of RIPA, just as they are more than capable of dealing with complex search warrant applications. Significantly, by virtue of paragraph 2(6)(b) and (8)(c) of Schedule 2 to RIPA, a magistrate can <u>already</u> grant appropriate permission when issuing a search warrant. I am conscious too that there is a limited number of District Judge courts. An amendment to paragraph 1(1)(a) of Schedule 2 to RIPA along these lines could also put the question of whether appropriate permission can be granted by a District Judge (magistrates' courts) beyond doubt.

699. I raise another related matter, given that the section 49 RIPA process has been described as "unnecessarily cumbersome". As observed, by virtue of paragraph 2(6)(b) and (8)(c) of Schedule 2 to RIPA, a magistrate can already grant appropriate permission when issuing a search warrant.

700. Imposing a RIPA notice on premises can facilitate access to devices and electronic data *in situ*. There are a host of reasons why it is in the interests of both investigators and suspects for law enforcement to obtain access to devices there and then on premises. Interrogating devices *in situ*, where feasible to do so, can allow investigators to either take away copies of relevant data or establish that a device contains no relevant data. Both instances may obviate the need for the seizure of entire devices. This is to the benefit of both investigators, who need not later triage and schedule devices, and suspects, who can retain these devices.

701. Search warrant application forms already prompt an applicant to consider and thereafter guide the applicant through the statutory conditions. I see sense in search warrant application forms being amended to (i) ask an applicant whether he or she intends to apply for appropriate permission to impose a disclosure requirement under section 49 of RIPA, and (ii) guide the applicant through the relevant statutory test.

702. **Insufficient deterrence** – Law enforcement agencies have additionally raised concern that the penalties set out in section 53 of RIPA are insufficient in deterring individuals from concealing their passwords, particularly those involved in serious and organised fraud. I have been told that suspects are routinely attempting to frustrate investigative proceeding by denying access to their devices and are willing to face judicial penalties instead of complying. This results in significant investigative delays and loss of critical evidence. Coupled with this is the concern over the lack of immediate consequences for failure to comply.

703. Section 53(5A) provides that the maximum penalty for knowingly failing to comply with a section 49 RIPA notice in a national security case or a child indecency case is five years and, in any other case, two years. I consider it appropriate for certain fraud offences for the maximum term to also be five years' imprisonment rather than two years'. I therefore recommend:

a. That section 53(5A)(a) of RIPA is amended so that the appropriate maximum term in a 'fraud case' is five years.

b. That subsections 53(8) and (9) of RIPA be inserted to define a 'fraud case' as a case in which the grounds, specified in the notice to which the offence relates, for imposing a disclosure requirement were, or included a belief that, the imposition of the requirement was necessary for the purpose of preventing or detecting an offence under any of the provisions listed in subsection (9). This is the same model adopted for child indecency cases.

704. **Failure to comply defences** – Law enforcement agencies have also raised concern that defendants are frustrating section 49 RIPA notices by simply claiming to have forgotten their passwords. "I forgot my password," so the argument goes, "and so I am not in possession of the key to the protected information and therefore have not knowingly failed to make the required disclosure." I am sympathetic to this concern of law enforcement. With that said, I am not of the view that reform to the defence provisions in section 53(1)-(4) of RIPA is necessary or desirable.

705. Section 53(4) of RIPA provides a defence where it was not reasonably practicable for a person to make the disclosure required but that he did make that disclosure as soon after that time as it was reasonably practicable for him to do so.

706. These provisions cannot, in my view, be tightened in a way which would prevent potential unfairness for a suspect. One cannot legislate that mere forgetfulness is not a defence. Section 53(3) of RIPA already places a reverse evidential burden in that regard. This could perhaps be raised to a reverse legal burden; however, the provision would then be susceptible to legal challenge on the grounds of Article 6 of the European Convention of Human Rights (ECHR). My final view is therefore that amendment to these provisions should not be made.

707. **Remotely stored data** – A final matter I consider, although not explicitly raised by law enforcement, is the position of remotely stored data. Above, I have set out the legal challenges which this material poses, particularly because of the presumption against extraterritoriality and international rules of comity.

708. The section 49 RIPA notice power "applies where any protected information has come into the possession of any person by means of the exercise of a statutory power … or is likely to do so". The drafter of this provision would not have had remote storage and cloud computing in mind. Technically speaking, where data is not stored locally on the device in question, but rather is accessible through an internet connection, that data will not have 'come into the possession' of the investigator. Notably, Police Scotland has published a document titled *Legal Basis for the Seizure and Examination of Digital Devices*, which states that their powers for the seizure and examination of digital devices apply "only to the contents of a device, commonly referred to as 'stored data' and not 'online data' accessed via that device".

709. The fact is that whether data is stored remotely rather than locally can be entirely arbitrary. It depends on the technical settings of a device, which may be unknown to the user of that device. Increasingly, devices and commercial products make use of remote data storage. Putting it in simple terms, it would be the highest degree unfortunate if a person, present in this jurisdiction, who created and accessed relevant data from a device in this jurisdiction, could resist an otherwise lawful section 49 RIPA notice because, unwittingly or not, data was stored remotely. Other than the characteristic of being stored remotely, there are no reasons for this material to enjoy a protected status in law. That should instead relate to the nature of the material, not its method of storage through a device.

Recommendation 22

To prevent otherwise lawful section 49 Regulation of Investigatory Powers Act 2000 (RIPA) notices being frustrated because relevant data is stored remotely rather than locally, it is recommended the Act be amended as follows:

a. References to protected information having come into the 'possession' of a person should include protected information not stored locally on the device but accessible through a network connection.

b. Paragraph 1(1)(a) of Schedule 2 should be amended to permit appropriate permission to be given by a lay justice.

c. Section 53(5A)(a) should be amended so that the appropriate maximum term in a 'fraud case' is five years, adopting the same model for child indecency cases by providing a list of relevant fraud offences which engage the increased appropriate maximum term.

Search warrant application forms should be amended to:

a. Ask an applicant whether he or she intends to apply for appropriate permission to impose a disclosure requirement under section 49 of RIPA.

b. Guide the applicant through the relevant statutory test.

Handling of Evidence

710. **Retention of digital information** – Fraud investigations are heavily reliant on digital evidence. Complex fraud investigations are frequently lengthy and take time to assess relevant evidence before a production order can be issued to seize it. The resulting loss of digital evidence across a range of harm types frequently hampers investigations and impairs their ability to successfully prosecute criminals.

711. In my initial report, *Disclosure in the Digital Age*, I discussed in depth the issues of handling data in high volume cases and advocated for the use of technology by officers to identify relevant material, as opposed to manually reviewing each piece of evidence.[472] This aims to streamline proceedings and narrow the focus on to relevant material.

Costs Protection in Restraint Proceedings

712. The Civil Procedure Rules impose a general principle that the losing party pays the legal costs of the successful party. This has a chilling effect on law enforcement, which may be deterred from pursuing high-value or complex cases due to the risk of adverse cost orders. Wealthy individuals, by contrast, can absorb such risks, creating a structural imbalance.

713. The Government has acknowledged this disparity. In its review,[473] of Part 5 of POCA it cited the *Perinpanathan* case,[474] which held that, where police or regulatory bodies act reasonably in pursuing a claim, there should be no presumption that they must pay the other party's costs. However, this principle applies only in magistrates' courts and does not extend to High Court proceedings, where most civil recovery cases are heard.

714. The Economic Crime (Transparency and Enforcement) Act 2022 amended the Unexplained Wealth Order (UWO) regime by introducing costs protection for enforcement agencies. Courts may now only award costs against agencies if they act

---

472 Home Office, *Disclosure in the Digital Age: Independent Review of Disclosure and Fraud Offences*, (2025), CP 1285, Recommendation 7a.

473 Home Office, *Report on the government review on introducing costs protections in civil recovery proceedings in the High Court under Part 5 of the Proceeds of Crime Act 2002*, (2024).

474 Ibid. citing R (Perinpanathan) v City of Westminster Magistrates' Court [2010] EWCA Civ 40.

unreasonably, dishonestly or improperly. Additionally, under the Crime and Policing Bill 2025, provisions have been included to introduce cost protection measures which will protect enforcement agencies from paying costs during civil recovery proceedings unless the authority is judged to have acted unreasonably, dishonestly or improperly.[475]

715. Restraint proceedings under Part 2 of POCA are governed by a separate costs regime. Section 52 of the Senior Courts Act 1981 provides that Rules of court may authorise the Crown Court to award costs and may regulate any matters relating to costs of proceedings in that court. Rule 45.7 governs the payment by a party of another party's costs on an application in restraint or receivership proceedings. Rule 45.7(6)(c) provides that the court must not order the prosecutor to pay the defendant's costs unless (i) the defendant succeeds, and (ii) the prosecutor acted unreasonably.

716. This is a welcome development which should encourage more ambitious enforcement and reduce the risk of agencies being financially penalised for acting in the public interest.

<u>Powers to Repatriate Assets</u>

717. A further recurring challenge in fraud investigations is the dissipation of assets beyond the jurisdiction, often within days of an investigation becoming known. While restraint orders under POCA are designed to freeze assets, their effectiveness is undermined if funds remain overseas, beyond the practical reach of enforcement agencies. Section 41(7) of POCA gives the court a broad discretion to make "such order as it believes is appropriate for the purpose of ensuring that the restraint order is effective". This power has long been interpreted to include repatriation orders, requiring defendants to bring movable assets back to the UK. In practice, however, the use of this power is inconsistent and often contested, despite its clear statutory basis and judicial recognition in cases such as *DPP v Scarlett*.[476]

718. Establishing a presumption in favour of repatriation in fraud cases would strengthen the integrity of restraint regimes and reduce the risk of assets being dissipated through opaque offshore structures. Fraud is inherently transnational, and the absence of a strong default position creates opportunities for delay and evasion. A rebuttable presumption, subject to compelling contrary reasons, would provide clarity, promote consistency, and align judicial practice with the underlying purpose of POCA: to preserve assets for confiscation and victim compensation. Without such a presumption, enforcement agencies face unnecessary litigation and uncertainty, which can erode the deterrent effect of asset recovery powers.

[475] Home Office, *Civil Recovery Cost Protections*, HC, vol. 766, debated on 30 April 2025.
[476] *DPP v Scarlett* [2000] 1 WLR 515 (Court of Appeal, Civil Division).

Recommendation 23

Establish a presumption in favour of use of the court's power under Section 41(7) of the Proceeds of Crime Act 2002 to make restraint orders in fraud cases, unless there is a compelling reason to oppose such an order.

14. International Cooperation

719. Having examined the United Kingdom's (UK) domestic powers to investigate and disrupt fraud, I now turn to the more complex challenge of transnational fraud. This is no longer a localised offence, it is global in scale, technologically advanced, and often driven by organised criminal networks operating across borders.

720. Tackling this threat requires coordinated international action. This chapter sets out the case for global cooperation between governments, international bodies and major corporations. The UK should lead in shaping this agenda, especially as artificial intelligence- (AI-) enabled crime emerges. Cooperation must be built not just on shared values, but on enforceable mechanisms that ensure accountability.

Setting the Scene

721. An estimated 70% of fraud has an international element, with 30% being primarily committed by overseas offenders.[477] Accordingly, if the problem of fraud is to be tackled effectively, international cooperation is vital. Whilst the need for enhanced domestic efforts taken to reduce the level of fraud is non-negotiable, the commitment of international actors to the reduction of fraud is of paramount importance. A cross-border response is required to tackle an international problem.

722. The prevalence of fraud is inextricably tied to the operations of transnational organised criminal gangs who have transformed fraud from the actions of a handful of rogues to an industrial scale model, replete with call-centres, online forums, and even fraud 'academies'.[478] This is without mention of the thousands trafficked and compelled to work in scam centres under the threat of violence and sexual abuse.[479]

723. The franchise model of fraud effectively enables independent or semi-independent operators to conduct scams and funnel their proceeds to senior leadership. This allows for the heads of these organised crime groups to recover from any potential losses, and to relocate and restart operations, if ever necessary.

724. Whilst it is common to refer to fraud threats as emanating from specific regions, a holistic image would stress the transnational nature of these operations. For example, scam centres in India have support groups "operating in the Gulf, China, Hong Kong, Uganda,

---

477 Home Office, *UK Government's approach to Fraud*, presented at the United Nations Office on Drugs and Crime Working Group on Technical Assistance (2025) [Accessed 30 September 2025].
478 Lazarus, S and Soares, A.B., 'From Business Centres to Hustle Kingdoms: Historical Perspectives on Innovative Models of Deviant Education', *International Annals of Criminology*, vol. 62, no. 3–4, 2024, pp. 449–468.
479 Office of the United Nations Human Rights High Commissioner, *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response*, (2023).

Canada, the USA and the UK".[480] Additionally, there are "accomplices in the target country (including the USA and the UK) who act as insiders and are necessary to get personal information on victims, move proceeds, and develop the scams".[481]

725. The dramatic evolution of international fraud is in no small part attributable to three key factors:

a. The proliferation of fraud-enabling technology.

b. A digital realm with sparse regulation.

c. Inadequate State responses.

Expansion of Technology

726. As noted in the chapter on fraud-enablers, the growth of technology has significantly lowered the bar for entry for fraudsters, granted a greater degree of anonymity, and allowed fraudsters to conduct their operations at scale. In the chapter 'Fraud Enablers and Connected Criminality', I further list technologies that have facilitated this international reach.[482]

727. Whilst fraudsters continue to adopt increasingly sophisticated technology, they are being countered by businesses employing similar tools to protect their finances and clients, and by law enforcement agencies leveraging cutting-edge technology to detect, disrupt and pursue fraudulent activity.[483] This constitutes a high-level game of cat and mouse, with law enforcement perpetually trying to pre-empt the different tactics fraudsters may deploy.

728. It is essential that governments, regulators, and industry leaders remain agile and forward-looking in their approach to technological innovation. This means not only investing in advanced tools to counter fraud, but also fostering collaboration across sectors to share intelligence, develop best practices and anticipate emerging threats. Without a coordinated and proactive response, the technological advantage will continue to favour fraudsters, leaving individuals, businesses and institutions increasingly vulnerable.

Moderating Online Spaces

729. Tied to this growth of technology is the development of social media, which has radically transformed society, enabling individuals from across the globe to connect with one another and often to find community. Whilst social media can play a powerful and

[480] Button, M., et al., *Scoping Study on Fraud Centres: Ghana, India and Nigeria*, (2024), page 21.
[481] Ibid.
[482] See chapter 'Fraud Enablers and Connected Criminality'.
[483] See chapter 'Short History of Fraud'.

positive role in supporting communities and independent journalism, it is increasingly being exploited by fraudsters to devise new schemes, identify potential victims and conduct targeted campaigns.

730. In an earlier chapter, I laid out the case for extending corporate criminal liability to social media companies and stressed the need for these platforms to moderate user generated content.[484]

731. It is important to recognise that social media companies exhibit similar behaviours to captured markets. Their values lie in everyone being on the same platform, which in turn makes it difficult for individuals to opt out or choose a competitor without losing access to the social connections or audience they had built. This contributes to users feeling locked into these platforms as their retention is almost structurally guaranteed. Proactive moderation, robust fraud detection systems, and transparent accountability mechanisms are not just best practices, they are essential obligations.

732. I recognise the inherent challenges posed by regulating social media companies, as they are large multinational corporations headquartered overseas. There is a limit to the UK's ability to enforce domestic standards or compel meaningful compliance with national laws. I have discussed several of these issues in the previous chapter, 'Corporate Responsibility'. Addressing the misuse of these platforms by fraudsters therefore requires not only robust domestic regulation but also coordinated international efforts to establish shared principles of accountability and digital governance.

Inadequate State Responses

733. The third factor contributing to the growth of fraud has been the inadequate and patchwork response of States to this growing global threat. Failures have ranged from lacking law-enforcement capacity, outdated technology, and siloed approaches. This has created an environment in which fraudsters can operate with relative impunity, exploiting regulatory gaps and jurisdictional fragmentation to avoid detection and accountability.

734. The Review heard evidence from law enforcement that fraud centres in priority jurisdictions are utilising a range of technology to avoid detection, automate and scale up their operations, and identify potential targets. The technology weaponised includes Voice over Internet Protocol (VoIP) servers, remote access tools (RATs), robo-diallers, and victim call lists which can be purchased through the dark web. After local law enforcement crackdown on larger scam centres, small-scale operations soon emerged.

735. An intelligence assessment on Southeast Asia suggests that fraud operations are industrialised in nature, with the convergence of skills in both technology and high-harm fraud threat types creating large, global scale reach. Activity is driven from established

[484] See chapter 'Corporate Liability'.

scam-compounds where trafficked and exploited individuals are enslaved on meeting targets against the number of victims engaged and or the amount of money stolen.

736. The Review also heard that operations in West Africa are smaller in nature than in Southeast Asia but larger in volume, often enabled by perpetrators working alone or in small affiliated groups. The fraud threat from West Africa is diverse, largely focused on investment frauds, romance frauds and sextortion, with the latter presenting a real risk to human life through culpable homicide.

737. To develop an effective fraud strategy, the UK must not only fortify its domestic defences but also play a leading role in strengthening global resilience, building consensus and addressing fraud at every level.

Building a Global Consensus

738. In a previous chapter, I discussed the inherent difficulties of international data-sharing.[485] I noted that the demand for a unified regulatory framework often clashed with the principle of State sovereignty. I turn now to look expansively at the UK's international strategy to address fraud, which must overcome a comparable challenge: securing international agreement on the urgency of fraud as a global threat and the need for coordinated responses.

739. To this end, the UK has taken several significant steps. On a multilateral level, the UK secured agreement on the first ever United Nations (UN) Resolution on Fraud, which was passed at the 12th Conference of Parties to the UN Convention on Transnational Organized Crime.[486] The resolution recognised fraud as an international issue in need of a unified response and an agreed shared terms on which it should be confronted.

740. Similarly, the Budapest Convention on Cybercrime, over two decades earlier, had provided foundational blueprints for countries seeking to develop domestic legislation on cybercrime and for international cooperation between state parties to this treaty.[487] In October 2025, the UN Convention Against Cybercrime sought to improve this standard and increase global outreach.[488] Whereas the Budapest Convention was a product of the Council of Europe and was not signed by major countries, such as China, India and Russia, the UN Convention is seen as more globally representative as it was negotiated by all UN member states. Importantly the convention expands the scope of the Budapest convention to specifically include threats such as cybercrime.

485 See chapter 'Data-Sharing'.
486 United Nations Office on Drugs and Crime, *Resolution 12/2: Implementation of the provisions on technical assistance of the United Nations Convention against Transnational Organized Crime*, (2024).
487 Council of Europe, *Convention on Cybercrime*, (2001).
488 United Nations Office on Drugs and Crime, *United Nations Convention against Cybercrime*, (2025).

741. However, the convention has not been without controversy, with some commentators raising concerns over the absence of human rights safeguards.[489] The watering down of these provisions reflects the difficult nature of securing global consensus.

742. The UK has played a vital role in leading international efforts to create a global consensus on fraud. This includes hosting the first Global Fraud Summit,[490] with a second summit being hosted by the UN Office on Drugs and Crime (UNODC) and the International Criminal Police Organization (Interpol) in Vienna in March 2026, supported by the UK. These summits present a unique opportunity for global collaboration with partnering countries as well as leading technology companies, among other industry partners, to achieve a whole-system global approach.

743. These summits complement efforts by the UK to work with international companies to tackle fraud across a wide range of sectors. The UK's Joint Fraud Taskforce has enabled various lead corporations to collaborate with the Government in designing voluntary charters committing them to taking concrete action that will aid in the tackling of fraud.[491]

744. The UK also continues to work cooperatively with international enforcement agencies. This includes working with Interpol to fund their Global Financial Fraud Threat Assessment, the most comprehensive evaluation of the global fraud threat.[492] The UK has also provided funding for a second threat assessment to be published at the next Global Fraud Summit. I am encouraged by these active steps to improve global data-sharing and provide intelligence on the threat of fraud.

745. These are all valued steps in raising the profile of fraud at the global level; however, momentum must be maintained and converted into tangible progress. To that end, the UK should take the lead in developing a protocol to the United Nations Convention against Cybercrime, ensuring fraud is explicitly recognised as a priority. This would embed fraud within the architecture of global cybercrime enforcement, strengthen cross-border cooperation, and provide a clear legal basis for intelligence sharing and joint disruption operations. Without such a protocol, fraud risks remaining a secondary concern, despite its scale, systemic impact and increasing convergence with cyber-enabled crime.

Recommendation 24

The United Kingdom Government should take the lead in developing a protocol to the United Nations Convention against Cybercrime, ensuring fraud is recognised as a priority.

---

489 Steffaro, A., '[The U.S. and UN Cybercrime Convention: Progress, Concerns, and Uncertain Commitments]', blog, Centre for Cybersecurity Policy and Law, 22 November 2024.
490 Home Office, '[UK hosts world leaders for first Global Fraud Summit]', news story, 11 March 2024.
491 Home Office, '[Joint Fraud Taskforce]', (2025). [Accessed 15 December 2025].
492 Interpol, '[Financial Fraud assessment: A global threat boosted by technology]', news story, 11 March 2024.

Successes of International Collaboration

746. Building on the challenges outlined in the chapter on data-sharing between states, recent developments offer promising examples of practical collaboration. For instance, the UK shared Action Fraud reports with Nigerian authorities where a Nigerian connection was identified.[493] To enhance the effectiveness of this initiative, the UK Government is now refining its approach by limiting shared information to clear, actionable data. This adjustment aims to reduce the administrative burden on Nigerian agencies while maintaining the integrity of cross-border cooperation. Initiatives like this not only strengthen bilateral intelligence on fraud but also lay the groundwork for more successful prosecutions.

747. The UK's multilateral collaboration with law enforcement agencies such as the European Union Agency for Law Enforcement Cooperation (Europol) and Interpol has also led to successful global counter-fraud operations such as Operation Stargrew[494] and Operation Elaborate.[495] The former was an international operation coordinated by Europol and supported by officers within the National Fraud Squad. The operation targeted Labhost, a web-based platform offering phishing services to criminals and used by around 2,000 fraudsters.[496] The operation resulted in 37 arrests[497] and enabled law enforcement to notify nearly 25,000 UK victims that their data had been compromised. This case illustrates the potential of coordinated, intelligence-led disruption to prevent further victimisation and dismantle criminal infrastructure.

748. These operations, collectively resulting in 179 arrests, underscore that international cooperation is indispensable to pursuing overseas fraudsters. They also demonstrate the value of liaison magistrates[498] and Crown Prosecution Service (CPS) Liaison Prosecutors[499] in explaining host-state law, shaping Letters of Request (LoRs) and extradition applications, and supporting efforts to identify and repatriate assets concealed abroad. Their role is facilitative: they help the UK to navigate foreign systems and to progress lawful requests efficiently.[500]

---

493 Home Office, 'UK-Nigeria partnership to detect, disrupt and deter fraud', news story, 1 May 2025.
494 Walsh, A., 'Joint searches conducted by international law enforcement and Gardaí to tackle organised fraud', Derry Now, 18 April 2024.
495 The Guardian, '100 people arrested in UK's biggest fraud investigation', (2022).
496 Sky News, 'Dozens arrested and thousands contacted after scammer site taken offline', 18 April 2024, [Accessed 25 November 2025].
497 BBC One Morning Live, 'Operation Stargrew', (2024), [Accessed 25 November 2025].
498 Liaison magistrates – judicial officers who act as a bridge between courts and external bodies (including international authorities) to facilitate judicial cooperation, ensure procedural compliance, and resolve cross-border issues. Their role is rooted in the judiciary and focuses on court processes.
499 Liaison prosecutors – are, by contrast, members of the prosecuting authority who coordinate investigations and prosecutions across jurisdictions, enabling evidence exchange and operational collaboration between domestic and foreign prosecutors. Their role is investigative and prosecutorial rather than judicial.
500 See chapter 'Powers' for a more detailed discussion.

749. Having heard detailed representations from the CPS, I am satisfied that delays in securing international assistance are not primarily a function of CPS resourcing. The principal impediments are the legal frameworks, sovereignty constraints and administrative capacity of partner jurisdictions. Where, for example, a state does not extradite its own nationals, or operates paper-based, multi-layered procedures for mutual legal assistance (MLA), appointing additional UK liaison prosecutors does not, of itself, remove the obstacle.

750. The more effective posture is earlier law-enforcement-to-law-enforcement engagement. From the outset of an investigation, an international strategy should be embedded, and routes should be channelled through a single UK front door, namely the Joint International Crime Centre (JICC), and the United Kingdom National Central Bureau (UK NCB) who should liaise Interpol and Europol liaison. Where judicial coordination is unavoidable, agencies should turn to the European Union Agency for Criminal Justice Cooperation (Eurojust) and, where appropriate, establish a Joint Investigation Team (JIT). CPS prosecutors should reserve LoRs/MLA for circumstances where judicial routes are strictly necessary.

751. It should also be recognised that the effectiveness of liaison officers remains contingent on the willingness and capability of host states to cooperate. Global fraud summits provide an opportunity to build consensus and to invest, through Foreign, Commonwealth & Development Office (FCDO) coordination, in targeted capacity-building within partner systems (for example, secure digital exchange, single points of contact and streamlined MLA practice), so that lawful cooperation can occur at pace.

<u>Building Capacity</u>

752. As previously noted, certain countries are struggling to tackle fraud within their borders, not out of ill-intent, but a lack of policing capacity. To this end, the UK should support initiatives which aid these countries in tackling fraud at its root. This may include support for multilateral institutions such as the UN, which provides a fraud toolkit with educational resources on tackling fraud as well as opportunities for donor coordination.[501] Alternatively, this could be more direct through bilateral police training on tackling fraud and on blockchain analysis. It is vital that the UK's efforts at tackling fraud are not limited to improving its own defences but directed to aid states in preventing and disrupting it at source.

<u>Issuing Sanctions</u>

753. Whilst there have been successful prosecutions of international fraudsters, they remain relatively rare. The process of gathering cross-border evidence and bringing cases to court is often lengthy, complex and resource-intensive. Although it is vital to pursue

[501] United Nations Office on Drugs and Crime, *Organized Fraud, Issue Paper*, (2024).

prosecutions to uphold justice and deter future offences, we must also consider complementary measures that deliver more immediate impact. These could include financial disruption, reputational consequences, and strategic deterrence mechanisms that do not rely solely on criminal conviction.

754. In a similar vein to the international money-laundering regime, the Government should explore the creation of an international fraud sanctions regime. Such a framework could allow for the designation of known fraudsters, enablers and associated entities—restricting their access to financial systems, freezing assets and limiting their ability to operate across borders. This approach mirrors existing models used to combat money laundering and terrorism financing, such as those developed under the Financial Action Task Force (FATF)[502] and implemented through the UK's Sanctions and Anti-Money Laundering Act 2018.[503] It would also align with broader efforts to reduce illicit financial flows under the UN Global Programme against Money Laundering[504] and the EU's Sixth Anti-Money laundering Directive (6AMLD).[505]

755. The Government should consider other penalties that can be imposed on criminal foreign nationals without requiring a full court proceeding. This may include the Home Secretary utilising immigration sanctions.

Recommendation 25

Designate foreign nationals orchestrating transnational fraud for targeted sanctions. This measure would enable the United Kingdom (UK) to impose asset freezes, travel bans and other penalties on individuals based overseas who coordinate or profit from large-scale fraud operations targeting UK citizens.

Recommendation 26

Deny United Kingdom (UK) visas from foreign nationals linked to fraud against UK victims, in line with existing powers under the Immigration Rules and the Sanctions and Anti-Money Laundering Act 2018. This complements the Government's use of targeted immigration sanctions against individuals involved in transnational criminal activity.

502 Financial Action Task Force, *FATF Recommendations*, (2025).
503 House of Commons Library, *The UK Sanctions Framework*, (2025).
504 UNODC, *Global Programme against Money Laundering*, (2016).
505 European Union, *Directive (EU) 2024/1640 of the European Parliament and of the Council*, (2025).

Addressing Non-Compliance

756. Much of what I have said is predicated on foreign support in the efforts to tackle international fraud. However, this support is not always forthcoming, and frequently corruption inhibits progress. Foreign governments may fail to prioritise the threat of fraud as it does not yet impact directly on their own citizens, or in certain cases, because they benefit from this illegal activity.

757. In countries such as Cambodia, the State draws benefit from the illicit activity of criminal gangs who often engage in human trafficking to establish scam centres.[506] Similarly, in Myanmar, these compounds do not benefit the State but are frequently located in territories held by ethnic armed organisations, outside of State control, and are lucrative for these militant organisations.[507]

758. Regardless of the motive, the UK must show leadership in this field and work to secure international cooperation. In recent years, the UK has embraced a transformative approach to free trade agreements (FTAs), moving beyond traditional concerns of market access and anticorruption to incorporate broader strategic and societal priorities. Drawing influence from pioneering agreements such as the United States–Mexico–Canada Agreement (USMCA) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which introduced enforceable chapters on anticorruption, gender equality, and innovation, the UK has begun embedding similar provisions into its own FTAs.

759. Post-Brexit trade policy has enabled the UK to include commitments on critical minerals, energy security, and inclusive economic development, reflecting a growing recognition that trade can be a vehicle for advancing national resilience and global values. This evolution signals a shift in trade philosophy, where economic liberalisation is increasingly aligned with geopolitical, environmental and social objectives.

760. Building on this momentum, similar treaty-based mechanisms could be leveraged to address anti-fraud measures, using transparency clauses, digital governance standards and cross-border cooperation frameworks to combat financial crime and protect public trust in global commerce.

Recommendation 27

Use trade agreements and memorandums of understanding to promote international law enforcement cooperation on evidence gathering, asset recovery, and extradition in fraud and economic crime cases affecting UK residents.

506 US Department of State, *2025 Trafficking in Persons Report*, (2025).
507 Australian Strategic Policy Institute, *Scamland Myanmar: how conflict and crime syndicates build a global fraud industry*, (2025).

761. In the chapter 'Corporate Liability', I explored further steps the Government could take to ensure that global corporations fulfil their obligations to combat fraud. This includes an expansion of failure-to-prevent fraud provisions to include user-generated content, as well as introducing an anti-fraud levy.

762. Even the most robust domestic fraud strategy will fall short if the UK remains exposed to global networks. Fraud is a transnational threat, fixing our own systems is necessary, but not sufficient. The challenge is not simply to defend our own, but to shape the global terrain, through diplomacy, enforcement and shared standards.

15. Prosecution

763. Having examined in detail the offences available to prosecutors[508] and the challenges of bringing fraud cases, particularly those involving large volumes of digital material[509]—I now turn to a related but distinct issue that arose frequently during my consultations: the growing role of private prosecutors in fraud. This chapter briefly explores the legal framework and the important role of non-State prosecutions, including their initiation, investigative powers, and the role in criminal proceedings.

764. Under Section 6(1) of the Prosecution of Offences Act 1985 (POA), any person can bring a private prosecution. This means individuals or organisations can bring criminal proceedings without investigations from the police or involvement from prosecuting authorities such as the Crown Prosecution Service (CPS) or the Serious Fraud Office (SFO). There are a small number of offences where the private prosecutor must seek consent from the Attorney General or Director of Public Prosecutions (DPP) or a Government minister before commencing a prosecution.

765. The DPP also has the power to take over any private prosecution under Section 6 (2) of POA and either continue or stop proceedings entirely. Whilst individuals could have this decision judicially reviewed, this can only be done if that decision is based on an unlawful application of the provisions of the Code for Crown Prosecutors, which governs the decision to prosecute.

766. In a private prosecution, the complainant assumes responsibility for all aspects of the case, from investigation through to trial. Funding is typically provided by the party bringing the prosecution. Although it is worth noting that section 17 of POA provides for the recovery of costs from central funds, either upon conviction or in confiscation proceedings.

767. Private prosecutors are subject to the Criminal Procedure Rules 2020,[510] which set out the relevant rules for bringing a prosecution in the magistrates' court and Crown Court. They are also subject to disclosure obligations under the Criminal Procedure and Investigations Act 1996 (CPIA). However, and as discussed in *Disclosure in the Digital Age*, private prosecutors and investigators must only 'have regard' to the CPIA Code of Practice, but are not bound like their Crown counterparts.[511] *The case of Hamilton & Ors. v Post Office*

[508] Home Office, *Disclosure in the Digital Age: Independent Review of Disclosure and Fraud Offences*, (2025), CP 1285, paras 307–309.
[509] See chapter 'Legislative Landscape'.
[510] *The Criminal Procedure Rules 2020*.
[511] Home Office, *Disclosure in the Digital Age: Independent Review of Disclosure and Fraud Offences*, (2025), CP 1285, Chapter 3.3 Trial Preparation.

Limited (2021), also highlighted in the report, is illustrative of the risks posed by inadequate disclosure in private prosecutions.[512]

768. For CPS prosecutors, the decision to prosecute is governed by the Code for Crown Prosecutors, issued by the DPP under section 10 POA. This test, as outlined in the Code, ensures there is sufficient evidence to provide a realistic prospect of conviction, and it is in the public interest to prosecute before charging suspects directly. There is no application to the court, as the decision to charge sits with CPS.

769. There is currently no statutory requirement for private prosecutors to satisfy these tests. Whilst the Private Prosecutors' Association's *Code for Private Prosecutors*[513] recommends adherence to these standards as best practice, compliance is voluntary. To commence proceedings, a private prosecutor must first make an application for a summons to the magistrates' court.

770. The Criminal Procedure Rules require that an application for a summons concisely sets out the offence alleged, the grounds for asserting the defendant committed it, and any previous relevant applications or proceedings, accompanied by a declaration of truth.[514] The court will then decide whether to issue the summons. If the application is refused, the prosecutor may seek judicial review of the decision in the High Court; if successful, the refusal will be quashed and the application reconsidered.

771. A number of organisations act as private prosecutors in England and Wales, including train operating companies,[515] regulators and charities. There are notable examples of successful private prosecutions for fraud in the UK, demonstrating the power and effectiveness of this legal route when public authorities are unable to act.

772. In 2024, Macmillan Cancer Support successfully brought a private prosecution against four defendants who exploited a grant system used to support cancer patients facing financial hardship. Criminal proceedings began in November 2022, charging the group with conspiracy to defraud before the group ultimately pleaded guilty to money laundering under the Proceeds of Crime Act 2002 (POCA). Macmillan recovered nearly all the stolen funds.[516]

773. However, the success of private prosecutions for fraud can vary significantly. For many years, the Royal Society for the Prevention of Cruelty to Animals (RSPCA) investigated and privately prosecuted the majority of animal cruelty cases in England and Wales.

---

512 *Hamilton -v- Post Office judgment*, (2021).

513 Private Prosecutors' Association, *Code for Private Prosecutors*, (2022).

514 Criminal Procedure Rules 2020, Part 7, rules 7.2–7.3.

515 Criminal Justice Act 2003 (Specification of Relevant Prosecutors Order 2016) made provision for certain train companies to bring fare evasion prosecutions under the Regulation of Railways Act 1889.

516 Edmonds Marshall McMahon, *Charity Fraud Case Study*, (2024), R *(Macmillan Cancer Support) -v- Edna Da Silva Vieira (2024),* Southwark Crown Court*,* [Accessed 4 December 2025].

However, the organisation has seen sustained criticism over its use of private prosecutions. In 2012, the RSPCA's prosecution of members of the Heythrop Hunt attracted significant media and political attention.[517]

774. In a January 2013 parliamentary debate, MPs criticised the charity's approach to prosecutions. A 2016 Environment, Food and Rural Affairs Committee recognised the potential conflict of interest due to its combined role in investigations, prosecuting and campaigning.[518] The committee recommended the RSPCA prosecute only in exceptional cases.[519]

775. Since then, several RSPCA prosecutions have drawn public, and even judicial, criticism. In 2020, a Lincolnshire farmer was acquitted of animal cruelty charges and later awarded £20,000 for wrongful arrest. The judge expressed concern over the charity's role as a prosecutor, stating that the RSPCA had "become involved in matters that could have been left to the appropriate bodies".[520]

776. Just last year, an animal rescuer was cleared of all charges of animal welfare and neglect. Judge Pattinson criticised RSPCA witnesses for pursuing a hidden agenda and being overly eager to prosecute.[521] In 2021, the RSPCA announced it would step back from its prosecutorial role and transfer responsibility to the CPS.[522]

777. The Post Office Horizon Scandal represents another particularly significant example of the risks associated with private prosecutions. In this case, sub-postmasters were wrongfully prosecuted by the Post Office, as the private prosecutor, based on incorrect data from the Horizon IT system. The scale and severity of the concerns prompted the Justice Select Committee to launch a 2020 review on the effectiveness of safeguards governing private prosecutions.[523]

778. The Committee heard evidence on the discrepancy between the tests applied by the CPS and magistrates' courts at the summons stage and acknowledged the effectiveness of existing safeguards was contingent on the approach taken by the respective magistrate and legal team. The Committee recommended the strengthening of safeguards and in particular, a binding code of standards to apply to all private prosecutors and investigators.

---

517 RSPCA v Heythrop Hunt Ltd & Ors (2012).

518 Environment, Food and Rural Affairs Committee, *RSPCA should step back from prosecutions except in exceptional cases*, UK Parliament, (2016).

519 House of Commons Environment, Food and Rural Affairs Committee. *Animal Welfare in England: Domestic Pets.* Third Report of Session 2016–17, HC 117. (2016).

520 Lynne Wallis, *Farmer wrongfully arrested at behest of RSPCA wins £20k in court* (2023) [Accessed 25 November 2025].

521 Sian Darlington, *Landmark Acquittal of Kirsten Fock and Justice for Rescued Animals* (2024).

522 The Royal Society for the Prevention of Cruelty to Animals, *Getting justice for animals* [Accessed 25 November 2025].

523 House of Commons, *Justice Select Committee's Ninth Report of Session 2019–21, Private prosecutions: safeguards*, (2020), HC 497.

Private Fraud Prosecutions

779. I outline the above not merely to set out the current framework for private prosecutions and highlight recent landmark failings, but to frame their broader application, an application that is no less prevalent in fraud than in other areas.

780. Some of the main arguments I heard in favour of private prosecutions for fraud included the potential for swifter progress compared with public prosecutions, greater control for victims, and the opportunity to pursue justice when public authorities decline to act. I heard that victims report fraud in good faith and then wait months for an update, whilst private prosecutions can offer a more immediate route to redress. Nevertheless, the current framework is not without criticism.

Standards of Prosecutors

781. The review heard consistent concerns regarding the standard of private prosecutions, which do not appear to be isolated incidents. In particular, there were reports of investigative actions being conducted by private prosecutors that failed to meet the minimum standards expected by law enforcement and CPS prosecutions. These deficiencies led to evidential gaps and required various investigative tasks to be redone. Stakeholders also noted that these delays can alert perpetrators, giving them the opportunity to conceal evidence and potentially taint witness accounts.

782. There is a clear case for a more robust regulatory framework governing private prosecutions to avoid jeopardising cases. The introduction of a mandatory code of practice was widely supported, particularly given the varied experience and expertise of some private prosecutors.

783. Whilst examples of good practice do exist, such as voluntarily adhering to the Code for Crown Prosecutors, this is not universal. The Ministry of Justice's consultation on standards and accountability to improve the behaviour and practice of prosecutions is a welcome development, and I support the recommendation for mandatory training and regulation in this area.[524]

Threshold for Prosecutors

784. In addition, the current level of scrutiny applied to the evidential basis for private prosecutions is, in my view, insufficient. There is merit in imposing a clear duty of candour and targeted disclosure on private prosecutors at the summons application stage, consistent with common-law principles and the Attorney General's Guidelines on

[524] Ministry of Justice, *Oversight and regulation of private prosecutors in the criminal justice system consultation*, (2025).

Disclosure, to ensure that material adverse to the application is put squarely before the court.

785. As regards evidential sufficiency at the summons stage, the High Court has reiterated that issuing a summons is a judicial decision, not an administrative rubber-stamp. Magistrates must be satisfied that the allegation constitutes a recognised offence, that the essential ingredients are *prima facie* present, that the matter is within time and jurisdiction, and that the applicant has standing.

786. In R *(Kay) v Leeds Magistrates' Court*, the Administrative Court[525] described compliance with the duty of candour as the 'foundation stone' of the *ex parte* process; failure to disclose material facts can justify refusal or quashing of a summons. The principle was recently applied in *Whitehead v Westminster Magistrates' Court*,[526] where the court upheld a refusal to issue a summons because the application did not meet the *prima facie* threshold. These authorities support a calibrated pre-summons evidential and duty of candour for private prosecutors.

787. Private prosecutors are subject to the CPIA regime and to common-law disclosure duties. *The Attorney General's Guidelines* (2024) emphasise early, proactive disclosure planning, and *R v DPP ex p Lee*[527] confirms that fairness may require pre-CPIA disclosure in appropriate cases. The Private Prosecutors' Association Code now expects a Disclosure Management Document (DMD) even in magistrates' courts (unless disproportionate), to provide transparency and judicial confidence. Embedding these duties at the summons stage, by requiring a short DMD and an advocate's candid certificate addressing weaknesses and alternative inferences, would materially improve decision-making and reduce downstream abuse arguments.

788. Courts have stayed private prosecutions tainted by improper motives or disclosure failings. In *Morjaria v Westminster Magistrates' Court*[528] the case was struck out as an abuse of process where proceedings were used for civil leverage and disclosure was defective. Likewise, in *Asif v Ditta*,[529] the Court of Appeal upheld a stay after serious integrity concerns, including use of a proxy prosecutor. These decisions underscore the need for a front-loaded evidential and candour standard to protect process integrity, conserve court time and avoid crippling costs risks.

525 R (on the application of Kay) v Leeds Magistrates' Court [2018] EWHC 1233 (Admin).
526 Whitehead v Westminster Magistrates' Court [2024] EWHC 2868 (Admin).
527 R v DPP ex parte Lee [1999] 2 All ER 737 / [1999] 2 Cr App R 304.
528 R (Morjaria) v Westminster Magistrates' Court [2023] EWHC 2936 (Admin).
529 *Asif v Ditta* [2021] EWCA Crim 1091.

Conclusion

789. Private prosecutions remain an important safeguard within our justice system, offering victims a route to redress when public authorities cannot act. Many are conducted to a high standard and have delivered commendable outcomes. However, the concerns raised during this Review, particularly around consistency, disclosure and evidential thresholds, are serious and merit further scrutiny. I therefore welcome the Ministry of Justice's decision to undertake a detailed analysis of these issues, and I support its efforts to ensure that private prosecutions operate to clear, robust and transparent standards.

16. Courts

790. In this chapter, I examine how fraud cases progress through the courts and why that journey matters for the effectiveness of the justice system. I begin by outlining the principal routes, civil and criminal, through which these cases travel, before turning to the distinctive barriers encountered in the criminal courts. This analysis is not academic: timely access to justice is a cornerstone of public confidence, yet as the Independent Review of Criminal Courts (Part One) has highlighted, persistent delays and backlogs—most acute in criminal proceedings, are failing both victims and defendants. Understanding these structural weaknesses is essential to shaping reforms that deliver fair, efficient, and credible outcomes.[530]

Civil Courts

791. In civil courts, fraud is pursued as a civil wrong or 'tort'.[531] The goal is typically to recover financial losses or assets, rather than to punish the wrongdoer. Any individual, company or organisation that has suffered loss due to fraudulent conduct can bring a civil fraud claim. These are often pursued when criminal prosecution is unlikely or too slow, or when the claimant's main goal is financial recovery. In England and Wales, a typical civil fraud case will progress through the stages described below.

792. At the pre-action stage, the claimant, formerly titled the 'plaintiff', and the defendant can seek to resolve the dispute without the requirement to progress to court. The parties are expected to follow the pre-action protocols, which encourage early sharing of information. This may include the use of a Letter of Claim and the consideration of Alternative Dispute Resolution (ADR).[532]

793. If a pre-court resolution is not secured, then the claimant will file a claim form detailing the particulars of their case.[533] The defendant is then served with the claim and typically has 14 to 28 days to respond, with options including acknowledging the claim, filing a defence, filing a counterclaim, or admitting the claim.[534]

794. Civil fraud claims typically fall under one or more of the following legal bases:

a. **Fraudulent misrepresentation** – Where one party knowingly makes a false statement to induce another to act to their detriment.

530 Ref Part 1, page 22.
531 A tort is a civil wrong, other than a breach of contract, which the law provides a remedy for in the form of damages, *Torts (Interference with Goods) Act 1977, s.1*.
532 Ministry of Justice, *Practice Direction – Pre-Action Conduct and Protocols*, (2022).
533 Ministry of Justice, *Civil Procedure Rules, Rules and Directions*, Part 7, (2022).
534 Ibid. Part 15.

b. **Deceit** – A deliberate act of deception causing harm.

c. **Breach of fiduciary duty** – Where someone in a position of trust acts dishonestly.

d. **Unlawful means conspiracy** – Where two or more parties conspire to use unlawful means to cause loss to another.

e. **Knowing receipt or dishonest assistance** – In cases involving misappropriated assets or breach of trust.

795. Where the claim is contested, the case will be allocated to one of three tracks,[535] with a Directions Questionnaire completed by both parties:

a. Small Claims Track for claims under £10,000.

b. Fast Track for claims between £10,000 and £25,000.

c. Multi-Track for claims over £25,000 or for complex cases.

796. To establish a fair playing field, parties then share relevant documentation that has a bearing on the case, or that they may rely on, during the 'disclosure' phase. This includes a duty to make a reasonable search for relevant documents. Expert report and witness statements are prepared and exchanged.[536]

797. The case is subsequently heard by a judge, and each party presents their arguments and supporting evidence.[537] The length of the trial is determined by the number of witnesses, volume of material, use of expert evidence, and court availability. When the trial is complete, the presiding judge can issue a judgment immediately or reserve it for a future date.

798. A judgment issued by a civil court will first consider if the claim(s) can be upheld. The bar for such a decision is whether the claim can be proven on the balance of probabilities. A party may then wish to appeal the decision, but typically only does so with judicial permission.[538] The remedies available to civil courts will be discussed in the following chapter.

---

[535] Ibid. Part 26.
[536] Ibid. Part 31.
[537] Ibid. Part 32.
[538] Ibid. Part 52.

Civil Powers

799. Beyond these foundational causes of action lies a broader civil toolkit—one that extends well beyond compensatory claims and into preventive, protective, and public-interest measures. I set out the key apparatus below.

800. **Private civil action to recover loss** – Claimants may sue in deceit, fraudulent misrepresentation, dishonest assistance or knowing receipt to restore their position by damages, equitable compensation or restitution. Where urgency demands, the court's equitable jurisdiction, now reflected in Civil Procedure Rules (CPR) Part 25 and s.37 of the Senior Courts Act 1981 (SCA), permits powerful interim remedies to preserve assets or evidence (e.g. freezing injunctions and search orders).[539]

801. **Freezing injunctions (formerly 'Mareva injunctions')** – The modern 'freezing order' prevents dissipation of assets domestically or worldwide pending judgment; it is granted where just and convenient under s.37 SCA and governed procedurally by CPR Part 25 (which includes the model forms and safeguards). The jurisdiction was developed in the decisions in *Mareva* [540] and *Karageorgis* [541], and has since been described as 'revolutionising' civil litigation.

802. **Search orders (formerly 'Anton Piller')** – In truly exceptional cases, where there is a real possibility that vital evidence will be destroyed, the court may order a supervised entry to premises in order to preserve evidence. The jurisdiction derives from *Anton Piller KG v Manufacturing Processes Ltd* and is now codified as a 'search order' under CPR 25.15–25.19.[542]

803. **Third-party disclosure to identify wrongdoers and trace assets** – Two critical tools are Norwich Pharmacal orders (to compel an innocent third-party who is 'mixed up' in someone else's wrongdoing to reveal the wrongdoer's identity) and Bankers Trust orders (to trace misappropriated assets via third-party custodians such as banks or exchanges). Both are frequently sought at the outset of fraud litigation, often in tandem with freezing relief.[543]

804. **Directors' disqualification (civil route)** – Separately from any criminal conviction, the Secretary of State (via the Insolvency Service) may bring civil proceedings under s.6 of the Company Directors Disqualification Act 1986 (CDDA) (or accept a disqualification undertaking) where conduct renders a person unfit to manage a company; orders

[539] Senior Courts Act 1981, s.37; Civil Procedure Rules, Part 25 (Interim Remedies).
[540] Mareva Compania Naviera SA v International Bulkcarriers SA [1975] 2 Lloyd's Rep 509.
[541] Karageorgis v Karageorgis [1976] 3 All ER 398.
[542] *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55 (CA); CPR 25.1(1)(h), 25.15–25.19.
[543] Norwich Pharmacal Co v Customs and Excise Commissioners [1974] AC 133; Bankers Trust Co v Shapira [1980] 1 WLR 1274.

commonly extend up to 15 years. These are protective measures for the public and are not punitive.[544]

805. **Serious Crime Prevention Orders (SCPOs).** An SCPO is a civil order that may be imposed:

a. Post-conviction by the Crown Court.

b. Or standalone by the High Court on application by specified authorities (e.g. the Director of Public Prosecution or the Serious Fraud Office (SFO)) where the statutory test is met; breach is a criminal offence. SCPOs are used to disrupt future economic crime by restricting specified dealings, communications, travel, or financial activity.[545]

806. Whilst SCPOs are civil penalties, breaching such an order may result in criminal penalties, including imprisonment. However, I have heard that use of these orders is rare, given that they require substantial resources to monitor their adherence. A more detailed discussion is included in the chapter 'Penalties'.

807. **Civil recovery (Part 5 of the Proceeds of Crime Act 2002 (POCA)).** Where appropriate, enforcement authorities (e.g. the National Crime Agency, SFO, Financial Conduct Authority, HM Revenue and Customs, or Crown Prosecution Service) can pursue non-conviction-based recovery of property obtained through 'unlawful conduct' in the High Court, applying the civil standard of proof. The Home Office guidance encourages early consideration of civil powers in parallel with criminal investigations.[546]

Civil Route: Advantages and Trade-offs

808. **Speed and control** – Civil procedure offers rapid, targeted interim measures, often without notice, to stabilise a fraud case before assets or evidence vanish. Courts can grant freezing injunctions, search orders, imaging directions and interim payments, enabling effective case management from the outset.

809. **Preserving evidence and assets** – Search orders (formerly 'Anton Piller') remain exceptional but decisive where there is a real risk of destruction of evidence. Correctly supervised, they prevent the 'evidential bonfire' that can defeat justice. Freezing orders, domestic or worldwide, restrain dissipation and compel disclosure, ensuring any judgment is not rendered pyrrhic.

810. **Disclosure and scale** – Norwich Pharmacal and Bankers Trust orders allow claimants to unmask wrongdoers and trace assets through third parties, though cross-border use

[544] Company Directors Disqualification Act 1986, s.6; Insolvency Service, *Disqualification of Directors: Guidance* (2024).
[545] Serious Crime Act 2007, Part 1; CPS Legal Guidance: *Serious Crime Prevention Orders* (2023).
[546] Proceeds of Crime Act 2002, Part 5; Home Office, *Guidance under s.2A POCA* (2023).

demands care in order to avoid breaching foreign laws. Where victims are numerous, a Group Litigation Order under CPR 19.21–19.26 and Practice Direction 19B delivers consistency and cost control through a managed group register and test cases.

811. **Standard and cost** – Civil fraud is proved on the balance of probabilities, albeit with cogent evidence, allowing recovery even in the absence of a criminal conviction. The trade-offs are cost, by way of the 'loser pays' rule, undertakings for interim relief, and potential security for costs under CPR 25.26–25.27. Practitioners must also weigh the expense of compliance and the limits of cross-border enforcement.

Criminal Courts

812. Having outlined the civil justice route, I now turn to the criminal process. As with all criminal offences, every fraud case is first heard in a magistrates' court. In this initial hearing, defendants are typically asked to enter pleas to the offences with which they are charged. As the most frequently used fraud offences are either-way offences,[547] the lay bench or a District Judge will evaluate the seriousness and complexity of alleged offending, before determining if it should be retained in their jurisdiction. If it is proposed that the case is suitable for summary trial, the defendant is then given the choice to consent to be tried in the magistrates' court or elect to have a trial by jury in the Crown Court.

813. If retained, the case will be heard by magistrates or a District Judge but without a jury. A determination regarding retention is more likely to be positive if the following factors are present:

a. The total amount of money involved is relatively low (e.g. a few hundred or low thousands of pounds).

b. The facts are straightforward and do not involve complex financial arrangements.

c. The defendant has no or limited previous convictions.

d. The likely sentence falls within the magistrates' sentencing powers (currently up to 12 months' imprisonment for a single offence, or six months if the offence was committed before April 2022).

814. A pre-trial hearing may then be convened to cover matters including case management, bail hearings, disclosure of material, and legal arguments which may be made about admissibility of evidence or procedural issues.

815. Where fraud cases are deemed too serious or complex, or where the defendant so elects, they are sent to the Crown Court. A plea and trial preparation hearing (PTPH) is held, the

[547] See chapter 'Legislative Landscape'.

trial is scheduled, and pre-trial hearings are held before the case is tried before a judge and a jury.

816. In concluding the trial, the triers of fact (either the lay bench or District Judge in the magistrates' court, or the jury in the Crown Court) must determine if the prosecution has proved, so that they are sure that the defendant is guilty of the offence(s) charged. If they are sure, they convict the defendant. Upon conviction, the sentencing bench or judge will refer to the Sentencing Council's Fraud Guidelines, which provide a structured framework for determining the appropriate penalty.[548] The court will assess factors including the value of the fraud, the level of culpability of the defendant, the impact on victims, and any aggravating or mitigating features which apply. Sentences may range from fines or community orders to substantial custodial terms, the latter typically applying in cases involving high-value or sophisticated offending. Sentencing is discussed in greater in the following chapter.

817. A convicted defendant retains the right to appeal against conviction and/or sentence. Appeals from the magistrates' court are heard by the Crown Court, and they are a re-hearing of the case or the sentencing exercise. Appeals from the Crown Court are heard by the Court of Appeal (Criminal Division), which will consider whether the conviction is unsafe, or the sentence manifestly excessive or wrong in principle or law.[549]

Discussion

818. There are several barriers to the timely progression of fraud cases through the criminal courts. For less complex fraud offences, the principal hurdle is that they are not treated as a priority within the criminal justice system, often overshadowed by offences perceived to carry greater immediate harm.

819. In contrast, serious fraud cases face a distinct set of challenges. These can include vast quantities of digital material, intricate financial arrangements, and multi-jurisdictional elements, all of which have practical implications for disclosure burdens, trial length, jury management, judicial oversight, and the adequacy of courtroom technology. These factors combine to place considerable strain on the system, particularly in Crown Courts lacking specialist experience or infrastructure.

Disclosure

820. As examined in my first Report,[550] disclosure is the process of identifying and sharing unused material that may assist the defence or undermine the prosecution. In fraud

---

548 Sentencing Council, *Fraud*, effective from 1 October 2014.
549 Judiciary UK, *Guide to Proceedings in the Court of Appeal, Criminal Division*, (2023).
550 Home Office, *Disclosure in the Digital Age: Independent Review of Disclosure and Fraud Offences*, (2025), CP 1285.

prosecutions, this obligation has become a structural fault line. The sheer volume of digital material, emails, messaging apps, cloud storage, financial datasets, has exploded.

821. My Review noted that an average Serious Fraud Office case now contains around 5 million documents, creating a disclosure exercise that can take months or years.[551] This is not a marginal inconvenience: disclosure failings have caused major trials to collapse, wasted public funds, and eroded public confidence in justice. The Criminal Procedure and Investigations Act 1996 (CPIA) regime, designed for a paper age, is now creaking under the weight of the digital era.

822. Fraud cases are uniquely exposed because they are often document-heavy and multi-jurisdictional. Investigators must sift through terabytes of data, often with overlapping privilege and privacy issues. Defence teams, in turn, face delays that undermine fair trial rights. My previous Report highlighted that, in my view, disclosure is now the single greatest cause of delay in complex fraud trials, with some cases stalled for years before reaching a jury.

823. Having identified systemic weaknesses in the current disclosure regime, I recommend a suite of reforms designed to modernise practice and reduce the burden on law enforcement and the courts.[552] Chief among these are amending the CPIA and its Codes to reflect the digital age; introducing an Intensive Disclosure Regime for the most complex cases, with early judicial case management; mandating a technology-first approach, including artificial intelligence- (AI-) assisted review under national standards; embedding a culture shift through mandatory training for investigators, prosecutors and judges; and strengthening accountability through enhanced oversight and sanctions for disclosure failings. Collectively, these measures will move the dial and bring the disclosure regime into the modern era.

Systemic Deprioritisation

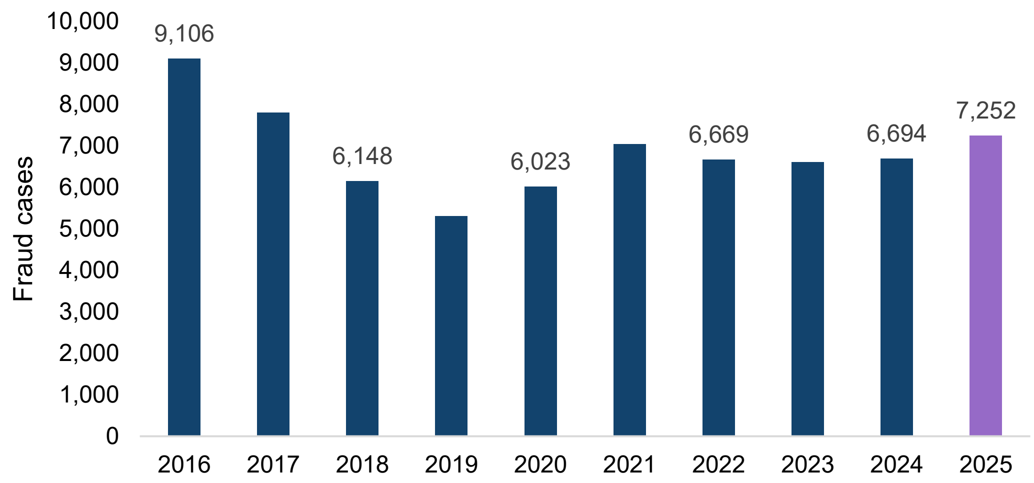
824. Furthermore, the evidence demonstrates that the systemic deprioritisation of fraud at the investigative stage persists throughout the criminal justice process and into the courts. At the time of writing, the magistrates' courts backlog stands at approximately 361,000 cases, while the Crown Court backlog has reached a record 78,000.[553] Every case caught in these queues is, in some way, impacted. Over time, evidence deteriorates, memories fade, witnesses disengage, and victims, faced with a drawn-out and often distressing process, frequently abandon their pursuit of justice.

825. However, these delays do not fall evenly across all crime types, and fraud is particularly disadvantaged. While data on the magistrates' backlog is limited, Crown Court figures

551 Ibid. Paragraph 242.
552 Ibid. Section 5, *Recommendations List*.
553 Ministry of Justice, *Criminal court statistics quarterly, April to June 2025,* (2025).

reveal a striking imbalance: although fraud accounted for only 1.8% of cases sent to the Crown Court in 2024,[554] it represents an estimated 9% of the entire backlog.[555] Equally troubling is the persistent trend of more serious fraud cases languishing for extended periods (see figure 12).[556] The Serious Fraud Office has provided evidence to this Review that shows, over the past three years, an average wait of 2.5 years between the date of charge to the start of a trial.

Fig.12 – High numbers of fraud cases in the Crown Court backlog



826. Some argue this reflects a failure at the investigative stage to generate sufficient quality cases for prosecution. While partly true, it does not explain why, once fraud cases reach the Crown Court, they are disproportionately overrepresented in the backlog. The reality is stark: almost one in every ten cases awaiting trial in the Crown Court involves a fraud victim and a defendant still waiting for resolution.

827. The Review received evidence from members of the judiciary and experienced legal practitioners concerning the practical constraints of court scheduling. It was observed that, due to mounting pressure to reduce case backlogs, there is a diminishing appetite within some court centres to list fraud trials of even average complexity, which may require several weeks to conclude. Instead, preference is often given to shorter, less document-heavy criminal cases that can be disposed of more swiftly. This operational reality may, in part, account for the growing number of fraud prosecutions languishing in the system.

---

554 Total Crown Court receipts in 2024 were estimated to be 121,601, with 2,160 of those being fraud cases.

555 Calculated using the number of fraud cases in the last full annual Crown Court backlog dataset 6,694 (2024), as a proportion of the latest Crown Court backlog total 76,957, (data published March 2025).

556 Data presented for 2025 as a **modelled estimate**, presuming the performance recorded in Q1 2025 is average to that of the remaining three quarters of 2025.

828. This pattern reflects a broader culture of deprioritisation. As noted earlier, fraud is often under-investigated; that neglect continues in the courtroom. Practitioners report that even straightforward fraud trials, once begun, are frequently adjourned in order to progress shorter, simpler cases. From a case management perspective, this may appear pragmatic. From the standpoint of justice, it is deeply unsatisfactory, particularly when considering the scale and societal impact of economic crime.

829. One factor contributing to these delays is the remand status of defendants. Unlike those charged with violent or high-risk offences, fraud defendants are typically granted bail, as they often pose neither an immediate physical threat to the public nor a significant flight risk. Consequently, their cases are not prioritised for early trial dates. Current data indicates that approximately 35% of all defendants are on bail, with fraud defendants disproportionately represented in this category.[557] While procedurally sound, this approach exacerbates delay and risks reinforcing the perception that fraud is treated with less urgency than other serious offences.

Judicial Training

830. Fraud cases are no longer confined to simple acts of deception. Increasingly, they involve multiple layers of technical and evidential complexity, driven by the rise of AI, cross-border fund transfers, and cryptocurrency. Tools once reserved for sophisticated criminals are now widely accessible, meaning magistrates and non-specialist Crown Court centres will face cases of a nature and scale they have not previously encountered.

831. For the most serious and complex trials, training is available through the Judicial College's 'Long and Complex Trials' course. However, this programme is optional and often overshadowed by courses on offences such as murder or sexual violence. As a result, judicial expertise in managing complex economic crime remains concentrated among a small cadre of judges in major cities. While efficient for those courts, this concentration limits the capacity of regional Crown Courts, which may lack both the experience and infrastructure to handle such cases effectively.

832. The Judicial College should review whether current and future judges are adequately equipped, or willing to develop expertise, in managing complex economic crime. This may involve expanding the scope of the existing course or introducing a dedicated programme focused on fraud and related offences. Consideration should also be given to mandating such training for judges likely to preside over complex fraud cases. Separately, and in light of the volume of fraud cases, it would be valuable for the wider judiciary to have a greater awareness of how to manage cases involving AI-enabled fraud and cryptocurrency-based money laundering.

---

[557] Ministry of Justice, *Criminal court statistics quarterly, April to June 2025,* (2025).

Recommendation 28

Invite the Judicial College to:

a. Review how best to prepare all judges, including magistrates, for the likely increase in hearing cases relating to artificial intelligence-enabled fraud and the laundering of money/assets using cryptocurrencies.

b. Review and update the existing 'Long and Complex Trials' course and to propose updating the training, or establish a bespoke module, covering the unique challenge of managing increasingly digital-heavy, serious and complex economic crime cases, and whether this training should be a requirement for all judges who hear complex economic crime.

<u>Preparation and Case Management</u>

833. Evidence from members of the judiciary and criminal justice partners reveals a persistent structural weakness: judges are not afforded sufficient time to master the detail of serious and complex fraud cases. The problem is acute where judges are transferred or parachuted in at short notice. Faced with vast volumes of digital and documentary material, they are expected to absorb and analyse the case at speed to maintain court timetables. That expectation is unrealistic and counter-productive: it undermines case management and, in practice, slows trial progression.

834. The difficulty is compounded by the obligation, under the *Goodyear*[558] principles, to provide an early indication of the likely maximum sentence should a defendant plead guilty. Where preparation time is inadequate, that duty becomes impracticable and risks eroding confidence in the process.

835. In my initial Report, I emphasised the need for robust judicial case management in material-heavy trials. I proposed an Intensive Disclosure Regime (IDR), under which judges scrutinise the prosecution case and defence critiques at the preliminary stage—specifically at the PTPH. That approach remains essential: it secures early engagement by all parties and resolves disclosure issues before trial. But it cannot operate unless the trial judge has been given time to master the relevant detail.

836. The principle is clear. If the judiciary is to exercise effective control over case progression and resolve disclosure disputes early, judges must be afforded adequate time to prepare.

837. A short, guaranteed period of pre-arraignment reading, coupled with early judicial allocation, is a modest investment that yields significant dividends: tighter and shorter lists of issues; a practical, well-signposted route to verdict; and materially firmer disclosure

[558] *R v Goodyear* **[2005] EWCA Crim 888**—on the **defendant's request**, a judge **may** give a sentence indication (normally the **maximum** on a guilty plea); the judge is **not obliged** to do so, it is usually given **after an agreed basis of plea**, and the indication **binds** that judge but **lapses** if a not-guilty plea is entered.

control from the outset. These gains translate into fewer interlocutory adjournments, more reliable *Goodyear* indications, and shorter trials through disciplined case management.

838. For these reasons, the following recommendation gives practical effect to this principle. A binding listing standard, early judicial allocation within four weeks of transfer, coupled with a protected week of uninterrupted pre-arraignment reading, ensures preparation is not eroded by operational pressures and delivers tangible benefits. It is a proportionate measure that promotes fairness, efficiency and public confidence, and it ought now to be adopted across Crown Court centres.

Recommendation 29

Judges assigned to preside over a serious or complex economic-crime trial (including fraud) should be allocated within four weeks of the case being transferred to the Crown Court. The allocated judge should then be afforded a minimum of one week's uninterrupted reading time before arraignment, to enable effective case management and the early resolution of disclosure issues. This standard should be embedded in judicial scheduling as a matter of principle, to secure fairness, efficiency and public confidence.

Court Proceedings

839. A clear opportunity for systemic improvement lies in the consistent adoption of best practice in the management of complex and lengthy fraud trials. Southwark Crown Court, widely recognised as the principal venue for serious economic crime, has taken a commendable lead in this area through the publication of a detailed note, *Judicial control and management of heavy fraud and other complex criminal cases*.[559] This document sets out a structured approach to case progression, designed to ensure that such trials are conducted with efficiency, fairness and judicial control. Having reviewed the Southwark Protocol, I am persuaded of its practical value and the clarity it brings to the conduct of serious fraud proceedings.

840. However, the Protocol's status is limited. It is not legally binding. As it expressly states, it does not create new rules or local practice but merely reminds practitioners of the manner in which judges might exercise their existing case management powers, and of the relevant provisions of the Criminal Procedure Rules and Criminal Practice Directions.[560] In short, it is guidance—not law.

[559] Southwark Crown Court, *Judicial control and management of heavy fraud and other complex criminal cases*, Practice note No.1/2024.
[560] Ministry of Justice, *Criminal Procedure Rules 2025 and Criminal Practice Directions 2023*, (2025).

841.

842. By contrast, a Practice Direction carries the force of law. Under section 74 of the Courts Act 2003, such directions may be issued only with the approval of the Lord Chancellor and the Lord or Lady Chief Justice. They sit alongside the Criminal Procedure Rules and are binding on all participants in criminal proceedings, including judges. Rule 1.2 of the Criminal Procedure Rules 2025 makes this explicit: all participants must comply with the Rules, Practice Directions, and directions of the court. The Court of Appeal has reaffirmed this position, most recently in *R v Brooker* [2024],[561] where it emphasised that compliance with these instruments is not optional but integral to the just conduct of proceedings.

843. The consequences of breaching a Practice Direction are materially different from those of disregarding a protocol. While not every breach will amount to contempt of court, certain provisions, such as those prohibiting unauthorised recording or premature disclosure of judgments, expressly state that violations may be treated as contempt. More broadly, non-compliance with a Practice Direction may result in a range of judicial sanctions, including adverse costs orders, the exclusion of evidence, or the adjournment or cancellation of hearings. These are significant powers, and their availability underscores the authority and enforceability of Practice Directions in a way that protocols cannot match.

844. Elevating the Southwark Protocol to the status of a Judicial Practice Direction would therefore have two significant effects. First, it would ensure consistent application of its provisions across all Crown Courts in England and Wales, all of which can hear serious fraud and economic crime, thereby addressing the current disparity in judicial approaches. Second, it would transform the Protocol's guidance into binding obligations, reinforcing judicial accountability and enabling courts to respond more robustly to non-compliance. Notably, the Protocol already contains provisions that impose duties on judges, for example, the requirement to maintain a detailed grasp of the case. Codifying such expectations within a Practice Direction would strengthen their enforceability and promote a culture of rigorous case management.

845. In light of these considerations, I recommend the Judicial Office to consider two related steps: first, the extension of the Southwark Protocol's application to all Crown Courts that hear serious fraud and economic crime; and second, its codification as a Judicial Practice Direction. These measures would not only promote consistency and efficiency but also signal the judiciary's commitment to improving the handling of economic crime at a time when such cases are becoming increasingly prevalent.

---

561 *R v Brooker* [2024] EWCA Crim 103.

Recommendation 30

The Judicial Office should extend the application of the Southwark Protocol to all Crown Courts across England and Wales that hear serious fraud and economic crime.

Recommendation 31

The Judicial Office should codify the Southwark Protocol into a Judicial Practice Direction to ensure consistent application across all Crown Courts.

Jury Trials

846. I turn now to a proposal which resurfaces whenever the system grapples with the burden of protracted fraud trials: the concept of judge-only hearings. At the time of writing, the Government has indicated its desire to pursue judge-only trials for fraud and the majority of other serious offences, excluding rape, murder, manslaughter and those in the public interest.[562] Advocates argue that such an approach could streamline proceedings, reduce cost and avoid the logistical strain of lengthy jury service. Critics, however, see it as a step toward dismantling a cornerstone of the criminal justice tradition. Both positions merit careful examination.

847. The Review heard strong and divergent views. The foremost concern was that replacing juries in serious fraud trials, simply for reasons of administrative convenience, would erode a fundamental safeguard of our system. Creating a carve-out for economic crime risks a two-tier justice model: jury for homicide and terrorism, but not for fraud, when the weight of the moral question is also heavy, has the defendant acted dishonestly to the criminal standard? The jury is not a ceremonial relic but a constitutional guardrail and a channel for public participation that confers legitimacy on outcomes affecting liberty and reputation.

848. Fraud prosecutions turn on dishonesty. The modern test assesses dishonesty by the standards of ordinary, decent people, not by professional or market custom. This points squarely to the jury as the proper tribunal of fact: if criminal liability depends on what the public would call dishonest, the soundest arbiter is a representative cross-section of the public applying clear directions and a structured route to verdict.

849. Proponents of judge-only trials contend that complexity and length justify reform. They argue that a single judge, steeped in forensic and commercial experience, could navigate intricate financial evidence more efficiently and deliver reasoned judgments that enhance transparency and appeal rights. Yet proposals to remove juries in 'serious and complex

[562] Ministry of Justice, *Criminal Court Reform*, Hansard, (2025), [Accessed 3 December 2025].

fraud' stumble at the threshold: there is no stable, principled definition of that category, nor a convincing reason to treat it differently from other lengthy and intricate cases. Many multi-handed murders, terrorism, grooming and drugs conspiracies take as long to try as a serious or complex fraud. Once complexity or length becomes the trigger, the logic spreads well beyond fraud.

850. The efficiency case remains unproven. Any perceived saving may be illusory: reasoned criminal judgments take time to craft to the criminal standard, and they would invite appeals comparing fact-finding 'methodologies' across different judicial approaches, creating a new field of litigation and simply shifting delay and cost upstream.

851. Experience shows juries cope when cases are properly managed and presented. Modern tools, the Criminal Procedure Rules and Practice Directions, disciplined case management, early judicial allocation, electronic evidence, focused schedules, and plain-English directions, have transformed trial presentation since the era of headline collapses. The real challenge is often length, not subject-matter complexity; this is addressed by realistic timetables, tight issues lists, and notes to juries detailing clear routes to verdict.

852. Public confidence matters. Trying fraud without a jury risks the perception of opacity or special treatment, particularly in high-profile economic cases of political interest. Jury trial keeps proceedings intelligible in open court to defendants, victims, the media and the public. Remove the jury, and that civic ownership of criminal justice is undermined. Also, it would feed the narrative that powerful defendants are judged behind closed professional doors.

853. Judge-only trials also carry practical hazards. In our adversarial system, judges routinely see prejudicial material when ruling on disclosure, bad character, hearsay and public-interest immunity; the same judge then becomes the sole fact-finder to the criminal standard. However professional the effort to compartmentalise, the appearance of bias is harder to dispel, and justice must be seen to be done. There are security and reputational risks too: a single named judge is indelibly associated with the verdict and cannot answer public criticism; a jury, by design, absorbs that heat.

854. Nor does a judge-with-assessors model fix the problem. It introduces fresh complexity (selection, diversity, remit, training and payment, among the issues), the danger of assessors importing untested professional norms into the fact-finding, and little prospect of time savings once deliberation and narrative judgment are added. On any sensible comparator, 12 citizens, diverse in background and experience, remain the safest tribunal for questions of honesty and credibility.

855. Claims about different conviction or acquittal rates before judges versus juries in fraud are anecdotal and methodologically weak. It is of course right that judges in the present system can accede to applications to dismiss charges and submissions of no case to

answer, where the relevant tests are met with reference to the evidence or lack thereof. No reliable, controlled evidence shows that changing the mode of trial improves accuracy or fairness; where outcomes differ, they usually reflect case selection and presentation, not the presence of a jury. The better course is to preserve jury trials for serious fraud and strengthen what already works: earlier and tighter case management, disclosure discipline, early judicial allocation ('cradle to grave'), clear written directions and visual aids, and realistic timetables. This path secures efficiency without sacrificing equality, legitimacy, or the public's stake in criminal justice.

856. Finally, the retention of jury trial for the most serious offences in the criminal lexicon but not for fraud would devalue the importance of fraudulent misconduct and reinforce the historic ambivalence towards fraud as a civil matter rather than a serious public wrong. This would be the wrong message for Parliament to send, in circumstances where the case for fundamental change in the manner of trial is not made out.

Court Infrastructure

857. Turning to the physical infrastructure of our criminal courts, it must be recognised that the presentation of evidence, particularly in fraud and economic crime trials, is now overwhelmingly digital. This shift is both inevitable and necessary, reflecting the nature of modern evidential material: voluminous, complex, and increasingly reliant on digital formats. Yet, despite this transformation, many court centres remain ill-equipped to meet the demands of such cases. Years of underinvestment have left numerous courtrooms without even basic, reliable audio-visual capabilities.[563] Stakeholders were candid in describing how trials are still routinely delayed or disrupted by technical failures at critical junctures.

858. In response, the Ministry of Justice told this Review that it launched the Digital Audio-Visual Evolution (DAVE) project in 2021 to modernise courtroom technology. A central feature is the Evidence Presentation System, which enables advocates to display digital material across all courtroom screens—ranging from wall-mounted displays to individual monitors for judges, witnesses, counsel and jurors. As of mid-2025, DAVE had upgraded 115 criminal courtrooms and 116 rooms across the wider court estate. With funding now secured for a further 90 courtrooms in 2025/26, the total number of DAVE-enabled crime courtrooms will rise to 205 by January 2026. The Review was told that the 80 rooms per year programme is now set to accelerate, subject to final spending approvals. This marks a positive step in the right direction.

859. Notwithstanding this progress, the reality on the ground remains uneven. The Crown Prosecution Service and some court centres continue to rely on third-party providers to deliver audio-visual services, often at considerable cost to the public purse. While some affordable providers exist, stakeholders expressed concern that the State is frequently

[563] The Law Society, *State of the courts: solicitors' views on the court infrastructure in 2025*, (2025).

paying a premium for functionality that ought to be standard in any modern courtroom. This is not merely a matter of convenience; it goes to the heart of the State's ability to prosecute serious crime effectively.

860. Fraud trials, in particular, are disproportionately affected by technological shortcomings. These cases often involve extensive digital exhibits, complex visual timelines, and multi-jurisdictional financial data. When audio-visual systems fail, the consequences are not trivial: trials may be adjourned, juries confused, and public confidence undermined.

861. More broadly, the condition of the court estate across England and Wales raises serious concerns. Many buildings are ageing, inflexible, and ill-suited to the demands of modern justice. The Court and Tribunal Design Guide,[564] updated in August 2025, sets out principles of accessibility, flexibility and sustainability. Yet, the real-world experience of court users often falls short of these aspirations. The physical environment in which justice is administered matters.

862. If the justice system is to meet the rising tide of complex economic crime, it must be underpinned by a court infrastructure that is fit for purpose. This means not only completing the DAVE rollout at pace but also ensuring that every Crown Court hearing serious fraud cases is equipped with the technology, space and support necessary to deliver justice effectively.

Recommendation 32

Invest in modern court technology infrastructure across England and Wales to support the effective trial of complex fraud cases.

Combining Civil and Criminal Courts

863. Infrastructure reform is not only about technology; it also raises structural questions about how we organise jurisdiction. The development of the new City of London Law Courts, expected to open in 2027, presents an opportunity to rethink how we handle complex economic crime. With 18 hearing rooms, including eight Crown, six civil and four magistrates' courts[565], this facility will inevitably become a focal point for major fraud and financial litigation.

864. The Review considered whether co-locating civil and criminal jurisdictions within a single centre could do more than improve logistics. Some have suggested a unified forum capable of addressing both criminal liability and related civil claims in a coordinated way.

[564] HM Courts & Tribunals Service, *Courts and tribunal design guide*, (2025).
[565] Bianca Castro, *£600m justice quarter marks building milestone*, (2025).

Proponents argue this could reduce duplication, accelerate asset recovery, and deliver a more coherent response to serious fraud.

865. The concept is not new. Lord Irvine of Lairg, in a 1998 lecture,[566] identified inefficiencies arising from multiple, sequential proceedings, criminal prosecutions, regulatory actions, and civil claims, each with overlapping facts but separate timetables. He proposed exploring a model where a single tribunal, with appropriate safeguards, could oversee these processes. Similar ideas have surfaced in past reviews, including Lord Justice Auld's Review of Criminal Courts in 2001[567] and the Attorney General Fraud Review 2006,[568] though the idea has never been implemented.

866. The theoretical benefits are clear: fewer delays, reduced costs, and a streamlined approach to disclosure and case management. A unified process could also mitigate the risk of breaching Article 6 of the European Convention on Human Rights by ensuring a fair hearing within a reasonable time. In principle, such a model could enhance efficiency without compromising fairness, if designed with robust procedural protections.

867. Whilst I recognise the potential efficiency of such a system, the underlying barriers to fraud investigations, the systemic deprioritisation of fraud, inadequate judicial training and inefficient case management, are not addressed. Without attending to these underlying obstacles, I fear that a unified system would continue to be plagued with the same inefficiencies as our current model.

868. Whilst this proposal is worthy of further consideration, and a potential pilot study, I would also encourage consideration of incremental reform as opposed to structural upheaval. One option, previously proposed, is to extend certain civil powers to the Crown Court in fraud cases. For example, judges already make Director Disqualification Orders under the Company Directors Disqualification Act 1986 following conviction, a measure designed to protect the public from unfit directors. This demonstrates that criminal courts already exercise powers with civil consequences, so extending their remit is not an unprecedented leap.

869. This proposal responds to a practical problem. During the Review, I was told of cases where convicted fraudsters were advised to dissolve the corporate entity through which the fraud was committed, only for the company to continue trading in another guise. This undermines deterrence and allows criminal enterprises to persist under a veneer of legitimacy.

870. Granting the Crown Court a statutory power to wind up such companies could close this loophole. While winding-up is traditionally a civil remedy, its purpose here would be

566 Lord Irvine of Lairg , KPMG Lecture: The feasibility of a Unified Approach to proceedings arising out of major city fraud (1998).

567 Lord Justice Auld, *Review of the Criminal Courts of England and Wales*, (2001), chapter 9, para 52 (page 384).

568 Attorney General's Office, *Fraud Review*, (2006), pp. 185–192.

preventive rather than punitive, aligning with existing sentencing objectives. Any such power would need clear statutory safeguards and appeal rights to ensure proportionality and fairness.

871. In summary, the new City of London Law Courts should be seen as an opportunity to modernise our approach to economic crime. A unified 'super court' remains, for now, a theoretical construct rather than a practical recommendation. The immediate priority should be targeted reforms, such as enhanced Crown Court powers, that strengthen the coherence and effectiveness of fraud prosecutions without compromising fundamental principles of fairness and transparency.

Recommendation 33

Extend civil powers already available to the Crown Courts, namely provisions under section 2 of the Company Directors Disqualification Act 1986, to enable courts to wind up a company explicitly being used, by a defendant, to commit fraud. Such powers would complement the introduction of a Criminal Receivership Order to strengthen the enforcement of financial penalties and asset recovery in economic crime cases (as proposed in Recommendation 3.9 of the Independent Sentencing Review).

Conclusion

872. This chapter began by asking how fraud cases progress through our courts and why that journey matters. Civil remedies offer speed and flexibility, but they cannot replace the public interest in criminal accountability. Yet in the criminal courts, systemic weaknesses, disclosure burdens, case management failures and inadequate infrastructure, threaten that imperative.

873. Some advocate novel solutions, from judge-only trials to unified 'super courts'. While these ideas merit debate, they carry profound constitutional and practical risks. The better course is targeted reform: modernising disclosure, strengthening judicial training, codifying best practice and investing in technology. Incremental innovations, such as extending certain civil powers to the Crown Court, could close loopholes without dismantling core principles.

874. If fraud is to be prosecuted effectively and fairly, the courts must be equipped for the realities of economic crime: digital evidence, complex financial structures and global reach. That requires sustained investment, procedural clarity and a reaffirmation of the values—fairness, transparency and public participation—that underpin our justice system.

17. Penalties and Remedies

875. The imposition of penalties in response to fraudulent conduct is a cornerstone of the criminal and civil justice systems of England and Wales. The legal framework governing such penalties is designed not merely to punish wrongdoing, but to serve a multifaceted purpose: to deter future offending, to rehabilitate the offender, to protect the public, to provide reparation to victims, and to express societal condemnation of criminal behaviour.

876. This chapter sets out the range of penalties and remedies available to the courts in cases of fraud, evaluates their effectiveness, and proposes reforms to ensure that the justice system responds proportionately and intelligently to the evolving nature of economic crime.

Criminal Penalties

877. As outlined in the previous chapter, criminal penalties are the result of a criminal prosecution where a defendant has been found guilty in a magistrates' court or Crown Court. Having made a determination of guilt, the court will then consider a range of factors in assessing the fairest and most effective penalties to impose.

878. **Imprisonment** – The most punitive penalty available to domestic criminal courts is the deprivation of someone's liberty by imprisonment. The five aims of sentencing are punishment, deterrence, rehabilitation, protection and reparation.[569] Incapacitation, the physical removal of a criminal from society, can significantly reduce a person's ability to continue offending. However, the rise of drone-facilitated smuggling[570] of technology and prohibited items into prisons means this is not a certainty.[571] In the context of fraud, imprisonment serves to reflect the seriousness of the offence, especially where it involves significant planning, breach of trust, or harm to victims.

879. As discussed in the chapter 'Legislative Landscape', central fraud offences such as the Fraud Act 2006, Conspiracy to Defraud, and Fraudulent Trading, all carry a maximum custodial sentence of ten years. Cheating the Public Revenue carries an unlimited maximum sentence, in practice, sentences of up to life imprisonment have been imposed in the most serious cases, though ten to 17 years are more typical for major frauds.[572]

---

[569] Sentencing Council, *General guideline: overarching principles*, effective from 1 October 2019.[Accessed 29 October 2025].
[570] BBC News, *BBC films drone dropping package into HMP Wandsworth*, (2025).
[571] HM Chief Inspector of Prisons, *Report on an unaccounted inspection of HMP Manchester*, (2025), page 20, paragraph 3.35.
[572] See chapter 'Legislative Landscape'.

880. The length of the custodial sentence is guided by the Sentencing Council's Guidelines for Fraud Offences,[573] which require courts to assess the offender's culpability, the harm caused or intended, and any aggravating or mitigating factors. These guidelines, discussed later, aim to provide consistency and proportionality in sentencing decisions.

881. **Community orders** – They offer a non-custodial alternative for less serious fraud offences or where the offender's circumstances make imprisonment inappropriate. They are governed by Part 12 of the Criminal Justice Act 2003. The aim of community orders is to rehabilitate the offender, protect the public, and punish through structured, supervised activity. They are structurally similar to suspended sentence orders, which are sentences of imprisonment, but which do not take effect immediately. Conditions may include:

a. Unpaid work (Community Payback).

b. Curfews or electronic monitoring.

c. Rehabilitation programmes (e.g. for substance misuse or financial management).

882. **Fines** – They are a financial penalty that can be imposed either in addition to, or instead of, imprisonment. Their primary aim is punishment and deterrence, particularly in cases where the offender has the means to pay. Fines are especially common in cases involving corporate offenders, where custodial sentences are not applicable.

883. Provision for such financial penalties is made under:

a. Magistrates' Courts Act 1980 (for summary offences).[574]

b. Powers of Criminal Courts (Sentencing) Act 2000.[575]

c. Criminal Justice Act 2003.[576]

884. In the Crown Court, fines can be unlimited in value, allowing the court to tailor the penalty to the seriousness of the offence and the offender's financial circumstances. The money collected from fines is paid into the Consolidated Fund, which is managed by HM Treasury and used for expenditure on a range of public services and Government functions.[577]

---

573 Sentencing Council, *Fraud*, effective from 1 October 2014.
574 Magistrates' Courts Act 1980, s.82 and s.85. Sentencing Act 2020, s.118.
575 Powers of Criminal Courts (Sentencing) Act 2000, s.130.
576 Criminal Justice Act 2003, s.164.
577 HM Treasury, *Consolidated Fund: Annual Report and Account 2023-24*, (2024).

885. **Confiscation Orders** – They are remedial rather than punitive. Their purpose is to deprive offenders of the financial benefit obtained through criminal conduct. These orders are governed by Part 2 of the Proceeds of Crime Act 2002 (POCA).[578]

886. Confiscation proceedings are initiated post-conviction, either at the request of the prosecutor or at the court's discretion. The court must determine:

   a. Whether the offender has a criminal lifestyle.

   b. Whether they have benefited from their criminal conduct.

   c. The recoverable amount based on their available assets.

887. If the offender fails to pay the amount ordered, they may face additional imprisonment by way of a 'default sentence'. The funds which are recovered are distributed through the Asset Recovery Incentivisation Scheme (ARIS), with portions allocated to law enforcement agencies, the Crown Prosecution Service, and the Home Office.[579]

888. **Compensation orders** – While confiscation orders are designed to deprive a defendant, compensation orders are a tool to compensate victims. These orders are designed to repay victims for the losses they have suffered because of a fraud. The application of such orders is governed by Sections 130–133 of the Powers of Criminal Courts (Sentencing) Act 2000.[580]

889. Courts are under a statutory duty to consider compensation before imposing fines or confiscation orders. This should ensure that victim restitution is prioritised in the sentencing process. Compensation is paid directly to the victim and can cover both financial loss and emotional distress, where appropriate.

890. **Criminal disqualification orders** – Under Section 2 of the Company Directors Disqualification Act 1986,[581] courts may impose disqualification orders on individuals convicted of fraud-related offences. These orders prohibit the individual from acting as a company director or being involved in company management for up to 15 years. The aim is to protect the public and the business community from individuals who have demonstrated dishonesty or unfitness to manage corporate affairs. Disqualification is particularly relevant in cases involving corporate fraud, false accounting, or abuse of fiduciary duty.

---

[578] Proceeds of Crime Act 2002, s.6.
[579] Of the total recovered monies, 50% is retained by the Home Office and the remaining 50% is distributed to law enforcement agencies and HM Courts & Tribunal Service, depending on the role played in the recovery process.
[580] Powers of Criminal Courts (Sentencing) Act 2000, ss.130–133.
[581] Company Directors Disqualification Act 1986, s.2

Civil Remedies

891. Civil courts in England and Wales have jurisdiction to impose a range of remedies in response to fraudulent conduct. These remedies are primarily compensatory or preventative in nature and are available to both private claimants and public authorities. Available remedies include the award of damages, injunctions to restrain further misconduct, declarations of legal rights, orders for restitution and, in appropriate cases, the transfer of profits obtained through fraud. In cases of non-compliance, the court may also impose sanctions for contempt.

892. **Fines** – The Public Authorities (Fraud, Error and Recovery) Act 2025 introduces a statutory civil penalty regime applicable to fraud committed against public authorities, including Government departments, local authorities and the National Health Service. Under Part 1 of the Bill, authorised officers of the Public Sector Fraud Authority (PSFA) are empowered to issue civil penalties without the need for a criminal conviction.

893. Civil penalties issued under the Bill are financial in nature and must be proportionate to the fraud committed. They are imposed on the civil standard of proof—namely, on the balance of probabilities. These penalties may be used in conjunction with debt recovery or criminal prosecution.

894. **Debt Recovery Orders** – These orders are available under POCA and the Public Authorities (Fraud, Error, and Recovery) Act 2025.[582] They enable the recovery of funds obtained through fraud, without requiring a criminal conviction. They may be enforced through civil proceedings or administrative mechanisms, including direct deductions from bank accounts or earnings via 'Pay As You Earn' (PAYE) mechanisms.[583] Public bodies such as HM Revenue and Customs (HMRC) and the Department for Work and Pensions (DWP) are permitted to use such powers.

895. **Injunctions and freezing orders** – As previously discussed, these may be granted under Section 37 of the Senior Courts Act 1981 and the Civil Procedure Rules.[584] These orders are used to prevent further fraudulent activity or to preserve assets, pending the outcome of proceedings. Freezing orders may apply to both domestic and international assets and are often sought at an early stage of investigation.

896. **Civil recovery of assets** – This is governed by Part 5 of the Proceeds of Crime Act 2002.[585] This allows the National Crime Agency and other designated authorities to recover property obtained through unlawful conduct. Proceedings are brought in the

582 Proceeds of Crime Act 2002, Part 2 & 5, Chapter 2, & Public Authorities (Fraud, Error, and Recovery) Act 2025, Part 1, Chapter 4, Section 17 ('Direct Deduction Orders').
583 Department for Work and Pensions, *Fraudsters face tougher action as Government gains new powers to tackle benefit fraud*, (2025), [Accessed 4 December 2025].
584 Senior Courts Act 1981, s.37; Civil Procedure Rules, Part 25.
585 Proceeds of Crime Act 2002, Part 5.

High Court and do not require a criminal conviction. Recovered assets may be sold to compensate victims or returned to the public purse.

897. **Administrative penalties** – These penalties are available under sector-specific legislation, including the Social Security Administration Act 1992 (for benefit fraud) and the Finance Acts (for tax fraud). They penalties are imposed by agencies such as DWP and HMRC and may include fixed penalties or percentage-based fines. They are typically used in lower-value or first-time fraud cases. The Public Authorities (Fraud, Error, and Recovery) Act 2025 also extends the limitation period for civil fraud actions to 12 years. This extension allows authorities additional time to investigate and pursue complex fraud cases that may not be immediately apparent.

898. **Serious crime prevention orders** (SCPOs) – They are civil orders, which can be imposed pre- and post-conviction. Most commonly, SCPOs are applied at the time of sentencing, following a criminal conviction, in the Crown Court, pursuant to Part 1 of the Serious Crime Act 2007.[586] Their purpose is to prevent the offender's involvement in future serious crime by placing restrictions on the individual or organisation. A breach of an SCPO is a criminal offence, punishable by up to five years' imprisonment. These orders are used in complex fraud cases involving organised networks or repeat offenders. Typical restrictions may include:

   a. Limits on financial transactions.

   b. Bans on certain business activities.

   c. Restrictions on communications or travel.

899. Alternatively, an application can be made to the High Court for a standalone pre-conviction SCPO, though in practice these are rarely made.[587] The court must be satisfied that the suspect has been involved in committing or facilitating serious offences. In evaluating an application, the court is focused on whether the suspect's conduct was objectively likely to facilitate serious crime and disregards their intent or mental state.[588] Currently, only the following agencies can apply for a pre-conviction SCPO:[589]

   a. Director of Public Prosecutions – England and Wales.

   b. Director of the Serious Fraud Office.

   c. Director of Public Prosecutions for Northern Ireland.

   d. Lord Advocate – Scotland.

---

586 Serious Crime Act 2007, Part 1, s.19 - *Di Maria v Commissioner of Police of the Metropolis & Others* [2025] EWHC 275 (Admin).
587 Crown Prosecution Service, *Serious Crime Prevention Orders* (2024).
588 Serious Crime Act 2007, s. 2(3).
589 Crown Prosecution Service, *Serious Crime Prevention Orders* (2024).

900. The Border Security, Asylum, and Immigration Act 2025[590] made amendments to the Serious Crime Act 2007, aimed at strengthening the effectiveness of SCPOs in tackling modern forms of serious and organised crime, including fraud and cybercrime. The reforms include the introduction of Interim SCPOs, enabling courts to impose temporary restrictions without notice where urgent preventative action is required. The Act also expanded the list of agencies authorised to apply directly to the High Court for an SCPO, now including HMRC, the National Crime Agency, British Transport Police, Ministry of Defence Police, and all police forces, not just in terrorism-related cases.

901. Further provisions include granting courts an express power to impose electronic monitoring (tagging) as a condition of an SCPO, and establishing a prescribed set of notification requirements to standardise the information collected from individuals and corporations subject to an order. These measures are designed to improve compliance monitoring, facilitate inter-agency coordination and enhance public protection.

902. Importantly, the Act also empowers the Crown Court to impose an SCPO following acquittal or appeal, where there is evidence of involvement in serious crime and reasonable grounds to believe that an order would prevent further offending. This two-limb test ensures proportionality while enabling preventative action in cases where a conviction is not secured but risk remains.

903. **Civil disqualification orders** – Separate from s.2 Company Directors Disqualification Act 1986 (CDDA) disqualification on conviction, the Secretary of State may pursue civil proceedings under s.6 CDDA (or accept undertakings) where a person's conduct renders them unfit; periods of two to 15 years are common. This is protective of the public rather than punitive and may proceed irrespective of any prosecution. As they are civil, rather than criminal proceedings, a criminal conviction is not required. Instead, courts make the order based on evidence of unfit conduct.[591]

Hybrid Penalties

904. **Deferred prosecution agreements** (DPAs) – They are a unique mechanism available under Schedule 17 of the Crime and Courts Act 2013.[592] The primary aim of a DPA is to encourage corporate accountability and reform while avoiding the collateral damage of a criminal conviction, such as job losses, reputational harm, or disruption to innocent stakeholders.

905. They are criminal in nature but allow corporate entities to avoid prosecution by agreeing to certain conditions. DPAs are currently only available to organisations, though the Independent Review of Criminal Courts has recommended that the scheme be extended

[590] Home Office, Border Security, Asylum and Immigration Act 2025, Part 3 – Prevention of serious crime.
[591] The Insolvency Service, *Company Directors Disqualification Act 1986 and failed companies*, (2025).
[592] Crime and Courts Act 2013, Sch. 17.

to individuals.[593] If an organisation complies with the agreed DPA terms, the prosecution is suspended and ultimately withdrawn. If not, the prosecution may resume. Terms may include:

a. Payment of fines.

b. Compensation to victims.

c. Implementation of compliance programmes.

d. Full cooperation with ongoing investigations.

Discussion

906. Plainly, both the criminal and civil courts have access to a range of penalties to choose from when deciding how to punish fraud offenders. However, in light of rising fraud offending and a decrease in successful prosecutions, it is not the number of penalty options that should be of concern, but rather their efficacy.

<u>Imprisonment</u>

907. The use of imprisonment in fraud cases remains one of the most visible expressions of the State's response to economic crime. The number of individuals prosecuted and convicted for fraud provides a quantitative measure of enforcement. However, it is the quality of sentencing outcomes, particularly their deterrent, rehabilitative and restorative effects, that must be the true metric of effectiveness.

908. In scrutinising the available data and listening to legal practitioners, two substantial criticisms of the current approach to fraud sentencing have arisen. Regarding first-time and low-level fraud offenders, there is a concern that short custodial sentences are setting individuals on a path to commit more serious fraud offending upon their release. Secondly, that maximum sentences available to courts, for the most serious fraud offenders, have failed to keep pace with other crime types and no longer reflect an offender's ability to steal significant sums of money and inflict untold misery on thousands of victims.

Lower-Level Offending

909. The term 'low-level fraud offending' is not defined in statute, but the Sentencing Council has provided guidance to the Crown and magistrates' courts to ensure sentencing remains proportionate.[594]

593 Ministry of Justice, *Independent Review of Criminal Courts Part 1*, (2025), recommendation 9.
594 Sentencing Council, *Fraud*, effective from 1 October 2014.

910. The guidance makes clear that sentencers should engage in a two-step process in which they first assess (i) the level of harm caused by the offence, this includes the intended and actual harm inflicted, and (ii) the culpability of the suspect. Consideration is then given to any mitigating factors such as a mental disability, difficult personal circumstances or significant remorse.

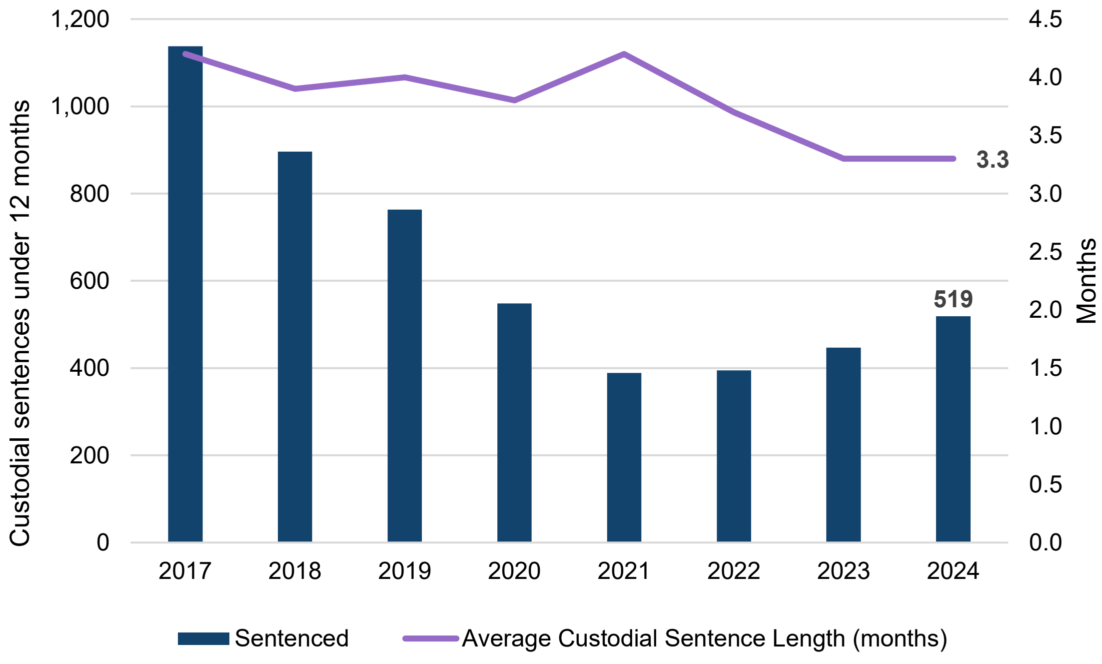
911. The lowest harm category considered, category 5, covers fraud in the ranges of £2,500 and £5,000. The guidance further notes that, where the offence had caused a risk of loss but no (or much less) actual loss occurred, there may be a case for considering the category below. However, this may not always be appropriate, particularly in cases where the risk of loss was high.

912. Beyond the financial harm, sentencers are advised to consider the impact on victims including emotional and psychological harm as well as factors which may make victims particularly vulnerable, such as their age or mental capacity.

913. Low levels of culpability are associated with the suspect being coerced, engaging in the offence opportunistically, limited awareness of the extent of fraudulent activity, or not being motivated by personal gain.

914. Last year, 519 fraud offenders were given custodial sentences under 12 months, with the average length for these sentences equating to approximately three months and nine days (see figure 13).[595] While there is no doubt that for a proportion of these individuals a short custodial sentence was the most appropriate penalty, there are also those for whom

Fig.13 – Frequent use of short sentences in fraud sentencing



595 Ministry of Justice, *Outcomes by offence tool*, Criminal court statistics quarterly: January to March 2025 publication.

imprisonment will only increase the likelihood of reoffending. This Review heard first-hand reports regarding the sharing of fraud techniques between inmates, which are subsequently employed to great effect upon release.

915. It is increasingly argued that short custodial sentences, particularly for first-time and lower-level fraud offenders, often do more harm than good.[596] Setting aside the current pressure on prison places, incarceration can provide a finishing school for criminality rather than places of rehabilitation. It is unlikely that imprisonment for a matter of months will provide sufficient time for meaningful education, though it may be long enough to fracture employment, housing, and family ties—key protective factors against future offending.

916. Worse still, short sentences for fraud offenders often delay the point at which an offender begins to face the real consequences of their actions: restitution, rehabilitation and reparation. When the system defaults to custody, victims can be left without redress, and the offender emerges more disconnected, with a greater understanding of how to commit fraud and therefore more likely to offend again.

917. There is also a broader systemic risk. If first-time fraud offenders perceive that the penalty for low-value offending is a brief custodial term, often served in overcrowded conditions with limited oversight, they may conclude that fraud is a low-risk, high-reward crime. This perception must be actively countered. The courts must be empowered to impose penalties that are swift, visible and constructive, without defaulting to incarceration.

918. Accordingly, this Review recommends that, where appropriate, first-time and low-level fraud offenders should not be given short custodial sentences. Instead, they should be diverted into alternative disposals that better serve the aims of punishment, deterrence and rehabilitation. These may include pre-court interventions (such as conditional cautions), robust community orders, financial reparation to victims, Deferred Prosecution Agreements, and mandatory attendance at fraud awareness or behaviour change programmes. These may also include the recommendation made by the Independent Sentencing Review, that the upper limit of Suspended Sentence Orders is extended from two years to three years.[597] This may have a significant impact on fraud offenders who fall into low-level and mid-level offending.

919. However, the effectiveness of such a recalibration depends on the speed and certainty of the justice system's response. At present, delays in investigation and prosecution mean that even low-level cases may take years to resolve. This undermines the immediacy of consequences and weakens public confidence. A justice system that responds quickly, proportionately and intelligently will not only deliver better outcomes for victims but will help to close the revolving door of low-level economic crime and custody. It is for these

[596] Mutebi, N & Brown, T. *The use of short prison sentences in England and Wales*, (2023).
[597] Ministry of Justice, *Independent Sentencing Review*, (2025).

reasons that I recommend that a pilot programme is devised to test a scheme which diverts those individuals who could benefit themselves and society by avoiding prison.

> **Recommendation 34**
>
> Pilot 'diversion from court' schemes for low-level fraud offenders, particularly where there is early admission of responsibility.

Mid-Level Offending

920. Turning next to mid-level offenders, who are implicated in higher levels of harm and culpability.

921. Medium culpability, as set out by the sentencing guidance, often corresponds to playing a significant role where offending is part of a group activity. The guidance makes clear that their culpability falls between higher and lower levels, which may include factors detailed in each tier.

922. In terms of financial harm, categories 2–4 may describe the level of harm, and concerns losses ranging from £5,000 to £500,000. This includes the intended and actual harm inflicted.[598]

923. There is limited evidence that current penalties provide a sufficient deterrent effect. Several factors contribute to the perception that fraud is a low-risk, high-reward crime:

   a. The low likelihood of prosecution.

   b. The lengthy duration of fraud case progression.

   c. The estimated custodial sentence.

924. **The low likelihood of prosecution** – As discussed in the chapter 'Contemporary Picture', a significant disparity exists between the volume of fraudulent conduct committed annually—now estimated at over 4 million offences[599]—and the number of individuals, 3,911 in 2024, who are convicted.[600] This gap is driven by a range of systemic challenges, including the significant proportion of international offenders and difficulties in attribution. Nevertheless, the broad decline in convictions further erodes the perceived credibility of the State's ability to hold fraudsters to account.[601] Fraud, already regarded as

---

598 Sentencing Council, *Fraud*, effective from 1 October 2014.
599 4.1 million incidents in the year ending June 2025 – Crime Survey England and Wales – Figure 1.
600 Ministry of Justice, *Outcomes by offence tool*, Criminal court statistics quarterly: January to March 2025 publication. Convicted for fraud as the primary offence.
601 See chapter 'Contemporary Picture', Figure 9.

less risky due to its often non-violent and remote nature, is now increasingly seen as a crime that is unlikely to result in any meaningful consequence.

925. **The lengthy duration of fraud case progression** – The deterrent value of a potential custodial sentence diminishes significantly when it is delayed by years.[602] The complex nature of fraud investigations and the volume of digital and financial evidence involved contributes to the glacial movement of fraud case to and through the criminal justice system. The overarching effect is that fraud cases are slow, resource-intensive and often frustrating for both victims and practitioners.

926. This Review heard from multiple stakeholders that the protracted nature of fraud proceedings encourages delay. Defendants who might otherwise consider an early guilty plea instead choose to contest charges, calculating that prosecution errors, resource constraints, or shifting public interest may lead to abandonment. In such circumstances, the threat of a custodial sentence ceases to function as an immediate or certain consequence. For many offenders, it becomes a remote and hypothetical risk, tomorrow's problem.

927. **The estimated custodial sentence** – Custodial sentences for all criminal offences have lengthened markedly over the past decade. Ministry of Justice data show that the average custodial sentence length (ACSL) for all offences rose from 13.7 months in 2010 to 20.9 months in 2023, an increase of approximately 53%. By contrast, fraud offences have experienced a far more modest rise. The ACSL for fraud increased by about 29% over the same period, with recent figures indicating an average of 22.9 months in the year ending March 2024, up from 20.1 months the previous year.[603] This divergence highlights that sentencing for fraud has not escalated in line with broader trends, raising concerns about its deterrent effect. At the same time, the number of successful prosecutions has declined, further weakening the perceived risk of committing fraud.

928. Taken together, these trends send the wrong message. They suggest that fraud is a crime with high rewards and minimal consequences. Without more consistent and visible penalties for mid-level offenders, the justice system will struggle to correct the perception of fraud as a lucrative and largely consequence-free endeavour.

Serious Offending

929. The third and most pressing concern raised by stakeholders in this Review relates to the adequacy of the statutory maximum sentence available under the Fraud Act 2006, currently capped at ten years' imprisonment. Even at its creation, this ceiling was considered inadequate by the Attorney General[604] and is increasingly viewed as insufficient

[602] See chapter 'Contemporary Picture'; Ministry of Justice, *End-to-end timeliness tool*, Criminal court statistics quarterly: January to March 2025

[603] Ministry of Justice, *Analysis of the change in average custodial sentence length from 2010 to 2023*, (2025), [Accessed 2 December 2025].

[604] Attorney General's Office, *Fraud Review*, (2006), paragraph 24-25.

to reflect the gravity of serious fraud offending. While many of the challenges outlined in the context of mid-level offending apply here, they are felt more acutely in cases involving high-value, complex and systemic fraud.

930. Serious fraud offending is characterised by high financial harm, extensive planning, abuse of trust and often systemic deception.[605] It may involve hundreds or thousands of victims, the use of corporate vehicles or digital platforms, and the concealment of assets across jurisdictions. Yet the courts are constrained by a sentencing ceiling that does not allow for proportionate punishment.

931. In practice, this Review heard that judges are forced to rely on consecutive sentences, default terms under confiscation orders, or alternative charges, such as money laundering, to arrive at a sentence that reflects the gravity of the offending.

932. Consecutive sentences are passed in alignment with the totality principle, which concerns the sentencing of individuals for multiple distinct offences. The totality principle maintains that the overall sentence must be just and proportionate, and that this cannot be reached "simply by adding together notional single sentences". The totality of each sentence is considered with a view to adjust downward to ensure the sentence is proportionate.

933. This stands in contrast to concurrent sentences, which are sentences served at the same time. Concurrent sentences are passed when the lead offence is insufficient to reflect the overall harm. Lesser offences are included with a view to adjust the sentence upward to reflect the totality of the offence, which may take the lead offence outside the category range appropriate for a single offence.

934. Sentencers are limited in their ability, as it is not permissible to impose consecutive sentences for offences committed in a single incident in order to exceed the statutory maximum penalty. Here the disparity between fraud and other economic offences is particularly stark. Cheating the Public Revenue, a common law offence, has no statutory limit and has attracted sentences of up to life imprisonment. Other harmful and serious offences, such as robbery and supplying Class A drugs, have a maximum sentence of life imprisonment.

935. I have noted that money laundering under POCA carries a similarly light maximum of just 14 years. As detailed in the cases below, these maximums are deeply unsatisfactory given the gravity of the harm caused. A serious fraudster or money launder may cause multi-million-pound losses, devastate lives and operate within an organised criminal network, but may receive penalties of no more than ten or 14 years and, under current release provisions, serve less than half that term.

[605] Sentencing Council, *Fraud*, effective from 1 October 2014.

Case study – LabHost (2025)

Zak Coyne, 24, headed up a platform, LabHost, which defrauded at least one million victims across the world, including 70,000 in the UK, of more than £100 million. LabHost itself made nearly £1 million (US $1.25 million) in profits from criminals.[606]

Mr Coyne was sentenced to eight and a half years. Currently, an offender serving this sentence would be released at the halfway point—around four years and three months. Under proposed reforms,[607] eligibility could shift to one-third of the term, about two years and ten months, subject to good behaviour and rehabilitation.

Case study – Bitcoin Cryptoqueen (2025)

Qian Zhimin, 47, masterminded an immense Ponzi scheme in China between 2014 and 2017, defrauding over 128,000 victims of approximately £5 billion. She laundered the proceeds by converting them into cryptocurrency, resulting in the largest confirmed Bitcoin seizure in UK history, over 61,000 Bitcoin.[608]

The presiding judge told the defendant she was "the architect of this offending from its inception to its conclusion ... [her] motive was one of pure greed".

Zhimin was sentenced at Southwark Crown Court to 11 years and eight months under the Proceeds of Crime Act (2002) for possessing and transferring criminal property. Currently, an offender serving this sentence would be released at the halfway point—around five years and ten months. Under proposed reforms, an offender could be released after roughly three years and 11 months.

936. The current workarounds are legally permissible but structurally unsatisfactory. They undermine transparency, distort charging decisions and erode public confidence. It remains crucial that judges can explain how a sentence is structured and how it has been calculated.

937. The case for reform is not merely comparative. It is grounded in the reality of fraud as the most prevalent crime in the UK. Victims suffer not only financial loss but emotional and psychological harm. Public trust in institutions is eroded. The economic impact is systemic. Despite this, the sentencing framework has remained static, failing to keep pace with the evolution of offending or the increase in societal harm.

938. Additional arguments for reform are rooted in the principle of judicial discretion. The current ceiling artificially constrains judges from tailoring sentences to the full range of culpability and harm. In cases involving abuse of public office, exploitation of vulnerable

606 BBC One Morning Live, 'Operation Stargrew', (2024), [Accessed 25 November 2025].
607 Ministry of Justice, *Independent Sentencing Review: Final report*, (2025), chapter four, Recommendation 4.1, page 57.
608 Han, T., 'Cryptoqueen who fled China for London mansion jailed over £5bn Bitcoin stash', (2025), BBC News, 11 November 2025, [Accessed 15 November 2025].

victims, or frauds exceeding £5 million, the inability to impose a sentence for fraud beyond ten years risks undermining the expressive function of sentencing, the ability of the court to mark the gravity of the offence in a way that is publicly intelligible and proportionate.

939. Moreover, the current framework fails to support the strategic aims of the justice system. Sentences that are perceived as lenient reduce the incentive for defendants to cooperate with law enforcement, return stolen assets, or plead guilty at an early stage. Raising the maximum would allow for a more meaningful discount regime, encouraging early resolution and restitution, discussed later.

940. It is important to emphasise that increasing the statutory maximum does not mandate longer sentences across the board. It simply restores judicial discretion in the most serious cases, where the facts warrant it. Data on long custodial sentences under the Fraud Act 2006 and POCA are limited. However, available indications suggest that, in recent years, no more than four individuals annually have received sentences exceeding eight years under the Fraud Act 2006, and no more than four have received sentences exceeding ten years for money laundering offences. Those who would qualify for the proposed new maximum are therefore likely to represent only a very small cohort of the most serious fraud offenders.[609]

941. Concerns about sentence inflation must be addressed directly. The proposed reform would be accompanied by updated sentencing guidelines, ensuring that proportionality and consistency remain central to judicial decision-making. The Sentencing Council would retain its role in calibrating starting points and ranges, thereby preventing any automatic escalation in sentence lengths for lower-level or mid-tier offences. It would also provide guidance on the levels of culpability and harm which would need to be demonstrated in order for an offender to attract a sentence close to the statutory maximum.

942. These reforms would also enhance the strategic value of cooperation agreements under sections 71 and 73 of the Serious Organised Crime and Police Act 2005. At present, the modest sentencing outcomes available in serious fraud cases limit the incentive for defendants to assist investigations. If trials are expedited and sentencing frameworks recalibrated, law enforcement agencies will be better placed to dismantle criminal networks and recover assets.

943. Whilst making this recommendation, I am aware of growing concern over sentence inflation. Too often, legislatures have sought to signify their law-and-order credentials by raising the length of custodial sentences. This has not been limited to serious offences but, as the Criminal Bar Association notes, has occurred "across the board". As the Gauke Review of Sentencing has shown, this often has unintended consequences, not limited to

[609] Ministry of Justice, *Outcomes by offence tool*, Criminal Justice System statistics quarterly: June 2025 publication.

increasing pressure on prison capacity.[610] I agree with his findings that Parliament should give serious consideration before recommending increases in sentences and must clarify the purpose for any such changes, particularly those over ten years.

944. In recommending the increase of fraud and money laundering sentences to a 20-year maximum, my principal argument is of proportionality. Given the scale of harm caused by fraud, the current sentencing regime is simply insufficient. Raising the maximum sentence ensures a proportionate punishment, and following from this will be a clear signal that such serious criminality will not be treated lightly.

945. This recommendation should apply to the most serious economic crime offences, namely: offences under the Fraud Act 2006 (including fraud by false representation, failure to disclose information, and abuse of position), conspiracy to defraud, fraud by false accounting, fraudulent trading under the Companies Act 2006, and money laundering offences under POCA. Each of these offences currently carries a statutory maximum of ten years or 14 years of imprisonment, well below the proposed 20-year ceiling.

946. Deciding on an exact number of years has never been straightforward. The sentencing guidelines emerged from a Victorian-era debate over whether prescriptive advice can be issued to the judges, or whether sentencing should be purely at a judge's discretion.[611] Given the absence of guidance during this era, there were widely disparate sentences; however, there slowly evolved common principles to ground sentencing judgments. Maximum sentences were typically determined by comparing similar offences and assessing the severity of harm caused, which in turn established historic precedents.

947. Today's maximum still reflects the fixed terms of punishment seen in the 18th century, when convicted prisoners were commonly sentenced to transportation to the colonies for set periods—typically seven years, fourteen years or for life.[612] [613] In moving away from this outmoded precedent, I maintain that 20 years is a reasonable maximum which allows headroom for judges to provide an appropriate sentence without being overly punitive.

Recommendation 35

Update the sentencing framework for serious fraud offences and money laundering, increasing the maximum custodial penalties to 20 years to reflect the gravity and impact of these crimes. It is for the Sentencing Council to review these proposals and to consider guidelines for sentencing for the most serious offenders.

---

610 Ministry of Justice, *Independent Sentencing Review: Final report*, (2025).
611 Roberts, J.V., et al., 'Sentencing Councils and Guidelines in the United Kingdom', in *Sentencing Guidelines and Commissions: Comparative Perspectives*, New York: 2025.
612 The Proceedings of the Old Bailey, *Punishment Sentences at the Old Bailey*, [Accessed 30 November 2025].
613 National Archives, *Criminal transportation*, Chapter 3, [Accessed 3 December 2025].

Greater Discounts for Early Guilty Pleas

948. The current framework for early guilty pleas in fraud and economic crime cases is governed by section 73 of the Sentencing Act 2020 and the Sentencing Council's guidelines, which typically allow for a maximum one-third reduction in sentence if a plea is entered at the earliest stage. While this structure provides a degree of consistency, it does not adequately reflect the complexity, cost and delay associated with prosecuting serious fraud.

949. In cases involving extensive digital evidence, international cooperation and multiple victims, the savings to the justice system from an early plea are substantial. Yet the incentive offered to defendants remains modest. This Review proposes a recalibrated approach, tailored to the realities of complex fraud.

950. First, the *Goodyear*[614] indication process should be reformed. Under current practice, the court may indicate the maximum sentence it would impose, if the defendant were to enter a guilty plea at the time of asking. However, this lacks precision; there should not be an indication that a guilty plea will make the difference between an immediate custodial sentence and a suspended sentence, for example.[615] This ambiguity may deter defendants from entering a plea. A revised model would permit judges to provide a specific sentence indication, subject to safeguards, where an early guilty plea is contemplated. It could also encourage indications as to the type of sentence; the difference between a sentence of immediate custody compared with a suspended sentence order may be significant to many defendants.

951. Second, the sentence discount itself should be increased. A significant reduction, for example of up to 50%, should be available for guilty pleas entered at the earliest opportunity, particularly in cases where the plea avoids a lengthy trial and facilitates victim compensation. Consideration should be given to whether the maximum amount of credit should be made available to the defendant at the plea and trial preparation hearing (PTPH), rather than only at their first appearance in the magistrates' court, on the basis that if a defendant has been sent for trial in the Crown Court or has elected as such, the PTPH is their first hearing in the venue which will try their case. In practice, there should be greater clarity on the nature and scale of the case against a defendant at this stage. This would reflect the strategic value of early admissions in complex economic crime.

952. These proposals would offer greater clarity and encourage early resolution; they sit together in the context of the recommendation to increase the statutory maximum sentences for fraud offences. The threat of greater penalties provides an incentive to engage with the revised *Goodyear* process, which of itself may encourage those inclined to plead guilty to do so at an earlier stage if it can be given in more specific terms. A plea is

---

[614] *R v Goodyear* [2005] 1 W.L.R. 2532.

[615] Archbold Criminal Pleading Evidence and Practice 2026 Edition, 5A-137; *Att.-Gen.'s Reference (*No.85 of 2014) (A) [2014] EWCA Crim 2088; [2015] 1 Cr. App. R. (S.) 14.

further incentivised by the greater reduction in sentence for a guilty plea. The result is a suite of incentives for defendants to accept guilt at an early stage or at all, which would have a positive, significant impact on the capacity of the court system.

953. Such reforms could significantly reduce the burden on court lists. Complex fraud trials often span months, consuming judicial resources and delaying justice for victims. By incentivising early pleas through clearer indications and meaningful discounts, the system can achieve faster resolutions, freeing capacity for other serious cases.

954. It is important to emphasise that these discounts would remain subject to judicial discretion and would not apply automatically. Safeguards would ensure that the seriousness of the offence and the interests of victims are properly weighed.

Recommendation 36

The Government should review and reform the current early guilty plea framework for complex fraud and economic crime cases. Specifically:

a. **Enhanced judicial indications** – Replace the current approach with a reformed *Goodyear* indication process, enabling judges to provide a specific sentence indication (rather than a broad range) should an early guilty plea be considered. This would give defendants greater clarity and incentivise early resolution.

b. **Increased sentence discount for very early pleas** – Introduce a significant sentence reduction for guilty pleas entered at the earliest opportunity, reflecting the significant savings in time and cost for the justice system and the benefit to victims.

Confiscation Repayment Incentives

955. The third proposal in this package is the creation of a further discount, for example up to 20%, where the defendant voluntarily returns property obtained through fraud. This would incentivise restitution and reinforce the principle that crime should not pay.

956. Under the current regime, confiscation orders are governed by Part 2 of POCA. Where a convicted defendant fails to pay the amount ordered within the specified period, the court may impose a default sentence—often substantial in length. This structure is punitive and designed to compel compliance. However, it operates retrospectively and does little to encourage proactive restitution.

957. This Review proposes a more creative and constructive model. Instead of relying solely on the threat of extended custody for non-payment, the system should offer positive

incentives for timely compliance. Specifically, where a defendant pays the full amount of a confiscation order within a defined period, say, 90 days, they should be eligible for a proportionate reduction in their custodial sentence.

958. This scheme is similar to the provisions which allow in principle a discount for an early guilty plea, and a reduction in sentence for an assisting offender. In the same way that these discounts are on a statutory footing, so should this regime be codified in Chapter 3 of the Sentencing Act 2020. This proposal is similar to the assisting offender regime and would benefit from mirroring section 74 of the Sentencing Act 2020, which gives the Crown Court, when determining sentence, the power to take into account the assistance offered or given. This regime has an accompanying safeguard; if a defendant fails to provide the assistance they agreed to provide, the prosecutor can refer the matter back to the Crown Court, which has the power to increase their sentence.[616] A new statutory provision should be created, in this part of the Sentencing Act 2020, following this format.

959. In the same way as the Sentencing Council has incorporated the statutory power to reduce sentences in light of guilty pleas within its sentencing regime, it would be well placed to remind and provide guidance to judges on the appropriate amount by which to reduce a sentence.

960. This approach would have several benefits:

   a. It would encourage rapid asset recovery, improving the likelihood of victim compensation.

   b. It would reduce enforcement costs and delays associated with non-payment proceedings.

   c. It would reinforce the principle of accountability, rewarding those who take steps to rectify the harm caused.

961. Concerns about fairness must be addressed. The incentive would apply only where the confiscation order reflects the defendant's realisable assets, as determined by the court. It would not advantage those with hidden wealth or penalise those unable to pay. Judicial oversight would ensure that the reduction is proportionate and does not undermine the seriousness of the offence.

962. For the avoidance of doubt, any reduction under this scheme should be discretionary and may be refused or scaled back where the court is satisfied that, prior to conviction, the defendant persistently resisted disclosure obligations or breached judicial directions, such that granting a full discount would undermine the interests of justice.

[616] Sentencing Act 2020, s.387.

963. Additionally, in cases where a defendant has entered an early guilty plea arrangement, and has been granted a discount on their sentence, the judiciary should be reminded to factor this in. This way, judges will be able to acknowledge the contrition displayed by the defendant, as well as their efforts to repatriate the proceeds of crime, but without granting an exorbitant discount which underplays the severity of their offence.

964. Ultimately, I am of the view that the incentive I have recommended will assist in reversing the emphasis in confiscation proceedings; instead of requiring payment and imprisoning individuals who do not pay, payment will be required and rewarded, within reason, if it is made in a timely manner. This would encourage faster asset recovery and improve victim compensation outcomes, which are both of paramount importance.

Recommendation 37

Introduce a statutory provision under Chapter 3 of the Sentencing Act 2020, mirroring section 74, which would enable discounted sentences where there is swift full payment of confiscation orders. This is in contrast to the current model of extending custodial sentences for delayed payment.

965. In progressing the recommendation to incentivise the repayment of criminal property, the Government will want to address a serious blind spot. Currently, no data is recorded for the number of individuals who are presently imprisoned because they have failed to satisfy a confiscation order. Although I am satisfied that my recommendation for an incentive to pay confiscation orders is appropriate, it would assist all stakeholders in the confiscation process to understand the rates at which default sentences are being imposed, the length of time served relative to the value of the outstanding award and, perhaps most importantly, the extent to which orders are repaid, even in part, after a person has finished serving their default sentence.

966. If the data reveals no improvement in repayment after the default sentence, it may be that the Government wishes to look more closely at the efficacy of imposing often lengthy default terms of imprisonment for non-payment.

Recommendation 38

The Ministry of Justice should begin systematically collecting and publishing data on the number of individuals imprisoned for failing to satisfy a confiscation order. This dataset should include a breakdown by the value of the order, using the following bands:

a. Less than £1 million.

b. £1 million–£5 million.

c. £5 million–£10 million.

d. More than £10 million.

Criminal Receivership

967. Fraud is a crime of calculated gain or deliberate loss, often involving complex asset structures, digital instruments, and rapid concealment. While POCA provides the statutory basis for confiscation and compensation, enforcement remains a persistent weakness. Where offenders fail to comply with court orders, the appointment of a Crown Court Receiver offers a powerful but underused remedy, particularly in high-value or evasive cases.

968. Receivership under POCA allows the court to appoint an officer to locate, manage and realise assets. However, practical challenges arise when assets include residential property. Seizing a defendant's home, especially where co-owners or dependents are involved, can be legally and emotionally fraught. Courts must navigate competing claims, establish beneficial ownership, and balance enforcement with fairness. Any expansion of receivership powers must be accompanied by clear judicial guidance on proportionality, third-party rights, and the treatment of primary residences.

969. The Independent Sentencing Review proposes a Criminal Receivership Order,[617] which could strengthen enforcement in economic crime cases. This would allow the Crown Court to appoint a receiver at sentencing, with powers tailored to the nature and location of the assets. To maintain public confidence, receivership must be used judiciously, with safeguards to ensure fairness, transparency, and accountability.

Deferred Prosecution Agreements

970. In recent years, there has been growing interest in the use of Deferred Prosecution Agreements (DPAs) as a tool not only for corporate accountability but for advancing justice in serious economic crime. Originally conceived as a mechanism to incentivise cooperation from individuals, DPAs have evolved into instruments primarily used between enforcement agencies and corporate entities. Their potential, however, remains underdeveloped, particularly in cases involving individual culpability.

971. Typically, a DPA involves a company admitting wrongdoing, agreeing to pay a financial penalty, and committing to certain conditions, such as compliance improvements or ongoing cooperation, with prosecution suspended so long as those conditions are met. Corporates, facing reputational and operational risk, often seek certainty and finality, making them more amenable to entering into such agreements.

[617] Ministry of Justice, *Independent Sentencing Review: Final report and proposals for reform*, Recommendation 3.9, pp. 51–52.

972. The Serious Fraud Office (SFO) has had notable success in securing DPAs with international companies, including Rolls-Royce,[618] Tesco,[619] and G4S.[620] However, its record in securing convictions against individual directors following these agreements has been poor. In the G4S case, the SFO dropped its prosecution against three former executives after ten years of investigation, citing "multi-faceted" reasons and acknowledging the "potential unfairness" of continuing proceedings.[621]

973. In pursuing Serco,[622] the SFO's prosecution of three individuals collapsed due to "insurmountable problems with its disclosure", despite the company having entered into a DPA to settle the allegations.[623]

974. The SFO has struggled to convert corporate admissions into individual accountability. Even its first DPA-related conviction, secured against a project manager who pleaded guilty to receiving bribes, was not for the conduct that formed the basis of the corporate DPA and came after a guilty plea rather than a contested trial. The collapse of trials, including the high-profile Serco case, has led to criticism that DPAs risk becoming a shield for individuals rather than a gateway to justice.

975. In light of the Independent Review of Criminal Courts' consideration[624] of deferred prosecution mechanisms for individuals, I believe there is merit in exploring whether a separate, court-supervised deferred prosecution mechanism should be created for named directors and senior employees in serious corporate economic crime cases.

976. Extending DPAs to named directors and senior employees would reinforce personal accountability, deter future misconduct and ensure that corporate cooperation does not operate as a shield for individual wrongdoing. Such agreements could be structured to include binding undertakings from directors, including disqualification from company management and the imposition of SCPOs. These conditions would be subject to judicial oversight and publicly sanctioned as part of the total resolution package.

977. Properly designed, individual DPAs could serve multiple purposes: they would incentivise early cooperation, facilitate asset recovery and reduce the burden on the courts. They would also allow for tailored sanctions that reflect both the gravity of the offence and the individual's role in the misconduct. Importantly, such agreements would not preclude prosecution in cases of non-compliance, nor would they dilute the seriousness of the

---

618 Serious Fraud Office v Rolls-Royce plc and Rolls-Royce Energy Systems Inc – Deferred Prosecution Agreement approved 17 January 2017.

619 *Serious Fraud Office v Tesco Stores Ltd* – Deferred Prosecution Agreement approved 10 April 2017.

620 Serious Fraud Office v G4S Care and Justice Services (UK) Ltd – Deferred Prosecution Agreement approved 17 July 2020.

621 Wilkinson, H. and Britton, J., 'G4S: Fraud trial against former executives dropped', (2023), BBC News, 10 March 2023.

622 *SFO v Serco Geografix Ltd* – Deferred Prosecution Agreement approved 4 July 2019.

623 R *v Woods and Marshall* (Southwark Crown Court, April 2021 – case discontinued).

624 Ministry of Justice, *Independent Review of the Criminal Courts: Part 1*, (2025), Recommendation 9.

offending. Rather, they would offer a structured and transparent alternative to contested proceedings, where the public interest is best served by resolution and reform.

978. I note that the concept of deferring prosecution is not new; courts at present have the power to bind over a defendant to keep the peace, and to defer sentencing for a period of time.[625] It is not suggested that either of these would be appropriate in the case of an individual involved in serious corporate wrongdoing, but rather that there is precedent for the proposal. In comparison to these powers, an individual DPA would allow for more tailored and onerous conditions imposed on such an individual.

Recommendation 39

The Government should consider creating a separate statutory, court-supervised deferred prosecution mechanism for directors, senior managers and, where justified, other employees materially implicated in serious corporate economic crime. Any such mechanism should operate alongside, and not in place of, corporate liability, and should be capable of incorporating appropriate preventative measures, including restrictions akin to serious crime prevention order measures, where proportionate.

Reinvesting Proceeds

979. The financial penalties secured through corporate DPAs represent a significant and largely untapped resource for reinvestment into the criminal justice system. Since their introduction, DPAs have generated hundreds of millions of pounds in fines, disgorgement, and cost recovery. In the Rolls-Royce case alone, the UK share of the settlement exceeded £239 million in financial penalties and £258 million in disgorgement. Tesco paid £128 million, and Airbus contributed over €980 million across fines and disgorgement.

980. To date, all of the SFO's DPAs have included terms which require the company to cover the costs of the SFO's investigation. The fine and any proceeds of the offending are paid into the Consolidated Fund, managed by HM Treasury. However, because DPA income is unpredictable and not forecast in advance, it is not earmarked for reinvestment. Instead, it is absorbed into general Government revenue. This represents a missed opportunity. Unlike fixed departmental budgets, DPA proceeds are extraordinary windfalls, generated directly through the enforcement of economic crime, and should be treated as such.

981. The case for ring-fencing a portion of DPA income for the criminal justice system is compelling. At present, almost every aspect of the criminal justice system is incontrovertibly under-resourced and desperate for additional funding. Even a modest allocation from DPA proceeds could support court maintenance, digital infrastructure, or

[625] Sentencing Act 2020 s.12, which preserves the power to bind over an offender to come up for judgment when called upon, and to defer sentence. The power to bind over an offender to keep the peace is a common law power.

specialist fraud units. These funds are not abstract—they are the direct product of wrongdoing, recovered through public effort, and should be reinvested to strengthen the institutions that made recovery possible. Further, the funds are not insignificant, the money secured under the Tesco agreement was equivalent to 11% of the annual criminal legal aid budget.[626]

982. Moreover, reinvestment would reinforce public confidence. Victims and taxpayers alike expect that penalties imposed for serious fraud will be used to improve justice outcomes, not simply absorbed into general expenditure. A transparent mechanism for allocating DPA funds to justice priorities would demonstrate accountability, support reform and ensure that enforcement success translates into systemic benefit.

983. In short, DPA proceeds should not be treated as incidental revenue. They are the dividends of justice, earned through investigation, negotiation and resolution. Their reinvestment into the justice system is not only logical but principled. I note that this recommendation should not reduce the regular funding which HM Treasury provides by way of the Spending Review process, but that fairness supports this recommendation in addition to the funding regimes already in place.

Recommendation 40

Proceeds of Deferred Prosecution Agreements should be injected into the criminal justice system and a proportion ring-fenced for economic crime enforcement activity.

Monitoring Deferred Prosecution Agreements

984. Having discussed the role of DPAs, it is worth examining the mechanisms undergirding these arrangements. As previously noted, DPAs are entered into on a voluntary basis with the company admitting to wrongdoing, agreeing to pay a financial penalty and committing to certain conditions. Since DPAs have been in use since 2014, most have expired without judicial intervention, indicating that either breaches were rare or were not pursued aggressively by prosecutors.

985. However, the SFO has recently taken legal action against Güralp Systems Ltd for allegedly breaching its DPA obligations—this includes failing to pay disgorgement, and poor compliance reporting. The case is ongoing, but early this year the High Court ruled that the SFO can enforce a DPA, despite the agreement ending in October 2024, if the terms of the agreement were not met.

[626] Serious Fraud Office, *SFO Deferred Prosecution Agreement with Tesco*, (2020).

986. This case raises an interesting question over the monitoring of compliance with DPAs. Currently, the SFO's powers under section 2 of the Criminal Justice Act 1987 (CJA) do not permit the agency to investigate potential breaches. Section 2(1) of CJA maintains that section 2 powers "shall be exercisable, but only for the purposes of an investigation under section 1". There is therefore a case for broadening the remit of its section 2 powers.

987. However, there are reservations about this proposal. In particular, there is concern a potential expansion of section 2 powers may have an adverse impact on perceptions of DPAs. Companies enter these arrangements to resolve criminal matters quickly and the prospect of continuous monitoring, even after finalising a DPA agreement, may disincentivise cooperation.

988. Furthermore, breaches of the DPA could be detected through stricter enforcement of terms set by the cooperation agreement. This may include a stricter payment schedule or ensuring that the participant complies with requests for disclosure.

989. Despite these reservations, the idea deserves greater consideration. However, any potential expansions of the SFO's powers must be proportionate and in line with obligations under the European Convention on Human Rights Article 8 rights of the recipient.[627]

Civil Protective Orders

990. The SCPO regime under the Serious Crime Act 2007 remains a powerful tool for managing high-risk offenders post-conviction or via High Court application. However, SCPOs are procedurally demanding, resource-intensive, and typically reserved for the most serious cases, often involving organised crime or multi-million-pound fraud. Their utility in addressing mid-tier or emerging economic crime is therefore limited.

991. By contrast, the civil protective order (CPO) regime under Part 4 of the Policing and Crime Act 2009, commonly associated with gang injunctions, offers a streamlined civil mechanism that could be adapted for fraud. These orders are granted on the balance of probabilities, without requiring a criminal conviction, and allow magistrates to impose tailored restrictions on individuals suspected of serious criminal conduct.

[627] Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, signed 4 November 1950, ETS No. 5, entered into force 3 September 1953. Article 8 of the European Convention on Human Rights protects the right to respect for private and family life, home and correspondence, subject to proportionate interference by public authorities in accordance with the law and as necessary in a democratic society.

992. Originally designed to curb gang-related violence, the framework could be extended to economic crime, enabling proportionate restrictions on those suspected of fraud-related activity. Conditions might include prohibiting the opening of new bank accounts, restricting involvement in company directorships, limiting access to encrypted communications, or requiring attendance at compliance programmes. Such measures would provide a flexible and preventative response to the enablers of fraud.

993. The advantages of this approach are clear. It would allow law enforcement to intervene earlier, reduce pressure on the Crown Court, and offer a scalable remedy for cases that do not yet meet the threshold for criminal prosecution. Operating within a civil framework, these orders would remain subject to judicial oversight and procedural safeguards, ensuring proportionality and fairness. They would not replace SCPOs but complement them, creating a continuum of powers that reflects the spectrum of economic crime. Evidence from gang injunctions suggests the deterrent effect of civil orders, with studies reporting significant reductions in offending and limited displacement of criminal activity.[628]

994. Introducing a fraud-specific CPO regime would require clear statutory criteria and safeguards to prevent misuse. Orders should be time-limited, subject to review, and integrated with existing enforcement tools such as confiscation powers under POCA and corporate liability provisions under the Economic Crime and Corporate Transparency Act 2023. With these protections in place, CPOs could become a vital instrument in the fight against fraud, one that prioritises prevention, reduces systemic strain and restores public confidence in the justice system's ability to act decisively.

Recommendation 41

The Government should legislate to create a fraud-specific civil protective order regime, modelled on Part 4 of the Policing and Crime Act 2009, empowering magistrates' courts to impose tailored restrictions on individuals suspected of minor fraud. This regime should include financial, business and digital activity controls, alongside positive compliance requirements, and operate within a framework of judicial oversight and proportionality.

Conclusion

995. The current penalty regime for fraud lacks the necessary deterrent effect. Fraud continues to be perceived as a low-risk, high-reward offence—particularly when compared with other serious crimes. This perception is reinforced by the belief that white-collar offenders are treated more leniently, which undermines public trust in the justice system.

[628] Carr, R. and Slothower, M., 'Do Gang Injunctions Reduce Violent Crime? Four Tests in Merseyside, UK', *Cambridge Journal of Evidence-Based Policing*, vol. 1, 2017, pp. 195–210.

996. Crucially, it is not only the penalties themselves but also the slow pace of justice that weakens their impact. Delays in investigation and prosecution diminish the immediacy and visibility of consequences, further eroding deterrence. Penalties are only as effective as their timely and consistent enforcement; without both, the system risks signalling tolerance for fraudulent behaviour. Reinforcing the five-fold purpose of penalties, punishment, deterrence, rehabilitation, protection and reparation, must remain central to reform. Only then can the justice system restore credibility and deliver proportionate responses to economic crime.

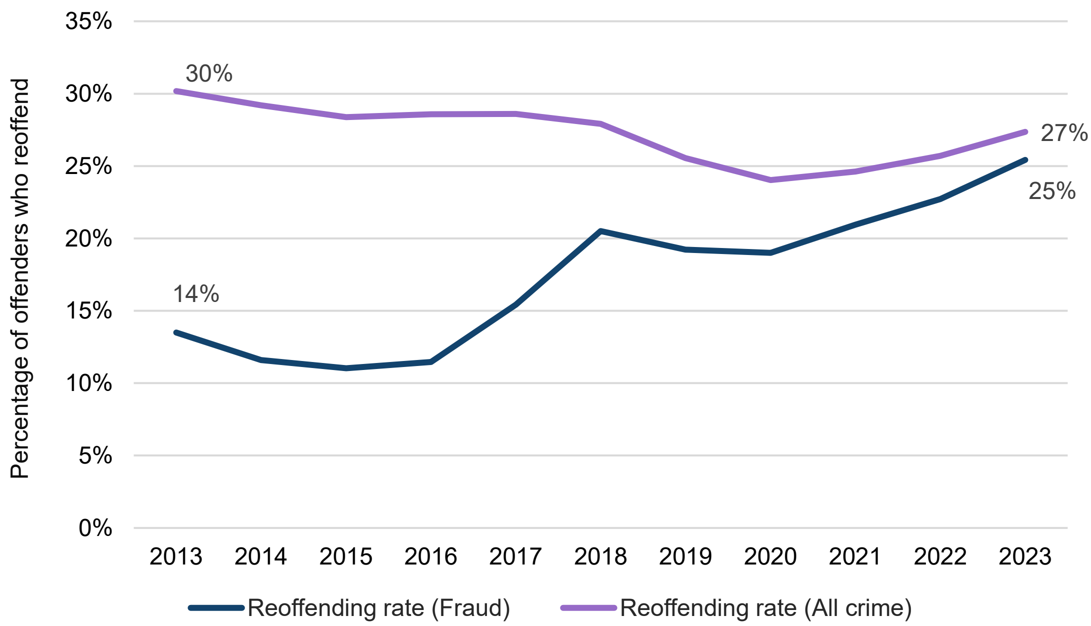
18. Rehabilitation

997. The preceding chapter examined penalties, but punishment alone cannot satisfy the full demands of justice. It is trite to observe that a modern criminal justice response must extend beyond retribution to encompass rehabilitation and victim support. Justice is not complete when the sentence ends; it must also seek to prevent future harm and restore confidence in the system. This chapter considers the potential of restorative justice as a rehabilitative tool in fraud cases, an approach that can reduce recidivism, promote accountability and give victims a meaningful voice in the process.

998. Current data underlines the urgency of this discussion. Rehabilitative interventions for fraud offenders appear increasingly ineffective. The most recent figures show that the fraud reoffending rate is rising and is now similar to the overall rate for all criminal offences: 25% compared with 27% in the year ending December 2023 (see figure 14).[629]

999. If the State is to adopt a genuinely proactive stance, it must look beyond detection, investigation, prosecution and punishment. A coherent plan is needed not only in relation to what happens after an offender leaves custody but also in relation to stopping them entering custody in the first place. Without this, the system risks perpetuating a cycle of reoffending—a costly and corrosive 'merry-go-round' that undermines both deterrence and public trust.

Fig.14 – Fraud reoffending rates now comparable to the average for all offences



[629] Ministry of Justice, *Proven reoffending statistics: October to December 2023*, year to December 2023, [Accessed 1 December 2025].

Restorative Justice: Principles and Practice

1000. Restorative justice models differ markedly around the world. At its heart, restorative justice brings those harmed by crime and those responsible for it into direct or indirect communication. The objective is to reflect on the offending and find a way forward. The communication is supported by one or more trained facilitators. It can be a way of disposing of a case without a prosecution, or it can be used alongside criminal proceedings.

1001. Domestically, it is more common for a restorative justice process to be used to divert a person away from the criminal justice system,[630] [631]but there is provision for restorative justice to be ordered as part of a deferred sentence under section 7 of the Sentencing Act 2020. Consent of all parties is required.[632] The Victims' Code of Practice, last updated early 2025, also contains a right of all victims to receive information about restorative justice from the police, and how to access services in the local area.[633]

1002. In the United Kingdom (UK), funding is available to all Police and Crime Commissioners for restorative justice, and all police areas publicly state that they provide access to local restorative justice services. The UK restorative justice model also proceeds on the basis that it can be used for any type of offence and at any stage of the criminal justice process but can only take place if both the victim and the offender consent to it.[634]

1003. The National Police Chiefs' Council has established three levels of restorative justice:[635]

a. **Level one** – Informal restorative justice, which often occurs as it happens (usually on the street), whereby police officers or police community support officers resolve low-level crime and anti-social behaviour. This can take the form of a community resolution, which includes the facilitation of on-the-spot discussions to defuse a situation immediately after a crime has occurred. The offender can apologise, and no further action is taken.

b. **Level two** – Restorative justice can be used instead of, or in addition to, the formal criminal justice process. It can be organised by police officers or staff for either a situation where a level-one resolution could not take place, or for more serious offences.

c. **Level three** – Will usually occur post-sentence but can also be used pre-sentence and can take place in prison. This may be for complex and sensitive cases where

630 Ministry of Justice, *Restorative Justice Action Plan for the Criminal Justice System for the Period to March 2018*, (2014).
631 Crown Prosecution Service. 'Out of Court Resolution: Restorative Justice' (2025).
632 Sentencing Act 2020, s 7(2).
633 Ministry of Justice, *Code of Practice for Victims of Crime in England and Wales (Victims' Code)*, (2025), paragraphs 3.4 and 3.5.
634 See, for example, Dorset Police 'Restorative justice' at https://www.dorset.police.uk/advice/advice-and-information/victim-support/restorative-justice/ [Accessed 30 October 2025].
635 National Police Chiefs' Council, 'Restorative Justice Evidence Briefing', (2022).

the offenders are prolific and must be monitored. All levels require facilitators who are experienced in restorative justice.

1004. The framework therefore appears to be established, but in practice access to restorative justice is inconsistent and the model not widely used. In 2021, the Restorative Justice All Party Parliamentary Group Inquiry into Restorative Practices called for a new Government action plan for restorative justice, as the last action plan expired in 2018 and the "sector has subsequently been lacking clear direction".[636] The Inquiry also found evidence that access to restorative justice was hindered by 'gatekeepers', where staff such as police and probation make decisions about the suitability of restorative justice despite lacking the skills or experience to do so. The Inquiry also called for the appointment of a Government minister with specific responsibility for restorative justice.

1005. Notwithstanding the 2021 Inquiry, problems with accessing restorative justice persist. In 2023, academics from the University of Nottingham and University of Gloucestershire[637] observed that there is a persistent gap between policy ambition and practical delivery. Despite its formal inclusion in multiple statutes, national action plans, the Victims' Code, and Government funding streams, restorative justice continues to function as an 'optional extra' within the criminal justice system.

1006. Further, the researchers noted that the 2018 Victims Strategy had proposed that Police and Crime Commissioners ensure restorative justice services are available, accessible and safe. However, this commitment has not been realised: the national action plan expired without renewal, funding is no longer earmarked, and victim awareness remains low. The Crime Survey for England and Wales reported that only 5.5% of victims were offered restorative justice in 2019/20, down from 8.7% in 2012/13.[638]

<u>Forms</u>

1007. Restorative justice encompasses a range of interventions aimed at constructive dialogue between victim and offender. It requires two-way communication, direct or indirect, and can proceed only where both parties consent and the offender accepts responsibility for the harm caused. Remorse or apology is not a prerequisite. The most recognised model is the victim–offender conference, a structured meeting led by a trained facilitator, often with supporters present. Community conferencing extends participation to those affected by the crime, while indirect communication—or 'shuttle restorative justice'—uses letters, video, or audio messages via a facilitator.

1008. Restorative justice also operates within statutory frameworks. For youth offenders, options include community resolutions, conditional cautions, referral orders and

---

[636] All Party Parliamentary Group on Restorative Justice, *Inquiry into Restorative Practices in 2021/2022*, (2021).
[637] Banwell-Moore, R. and Hobson, J., *Restorative Justice: summary of evidence and the current UK position*, (2023).
[638] Office for National Statistics, *Restorative justice, year ending March 2011 to year ending March 2020: Crime Survey for England and Wales (CSEW)*, (2020).

rehabilitation orders, each capable of incorporating restorative elements. Restorative justice may occur during or after custody and is increasingly used for early intervention in schools and communities. For adults, restorative justice is most often embedded in community resolutions or conditional cautions, and courts may defer sentence post-conviction to enable restorative justice activity. These mechanisms illustrate restorative justice's versatility: from informal resolutions to court-sanctioned conferences, it can address harm at every stage of the criminal process.

Victim Recovery and Satisfaction

1009. Restorative justice is not solely about offender reform. It is also a mechanism for victim rehabilitation. Victims of fraud often experience emotional distress, loss of trust, and a sense of invisibility within the justice process. Restorative justice offers a structured forum for victims to articulate harm, receive acknowledgement and regain agency.

1010. The College of Policing[639] and the Ministry of Justice[640] both cite restorative justice as effective in reducing reoffending and enhancing victim satisfaction. Victims report improved wellbeing, increased feelings of safety, and greater closure. A Ministry of Justice study found that restorative justice reduced reoffending by 14%, with 85% to 90% of victims satisfied with the process.[641]

1011. Taking a more macro view, there are signs that restorative justice could also be cost effective. An economic evaluation published in *Frontiers in Psychology* found that restorative justice yields a social return of £14 for every £1 invested, with a direct return of £4 to the criminal justice system.[642] There is potential for restorative justice to deliver real economic value, with any savings reinvested to support further victims of fraud.

Restorative Justice in Fraud: Emerging Practice

1012. There is limited empirical research on restorative justice in fraud cases, either in the UK or internationally. However, several UK examples illustrate its potential:

1013. **City of London Police trial (2017)** – The City of London Police, in conjunction with the Home Office, designed a restorative justice trial focused on insurance-fraud offenders. Offenders had made false claims and had few or no antecedents. The trial involved a mediation between the offender and the insurance company. The scope of the trial was considered "too limited to provide insight as to whether … restorative justice with low-level insurance fraudsters caused any long-term behavioural change in participants".

639 College of Policing, 'Restorative Justice: Evidence Briefing', (2022).
640 Ministry of Justice *Reducing Reoffending: A Synthesis of Evidence on Effectiveness of Interventions.* (2025).
641 Ibid.
642 Grimsey Jones, F., et al., 'An Economic Evaluation of Restorative Justice Post-Sentence in England and Wales', Frontiers in Psychology, 14:1162286, 2023.

1014. The trial was successful in enabling offenders to appreciate the impact of the offence on their victims and assisted them in understanding their own motivations. There was, accordingly, a case for "cautious optimism" that restorative justice may be a useful method of disposal for low-level fraud offences.[643]

1015. **Sussex Police case (2017)** – An employee who defrauded her employer of £150,000 over four years was sentenced to three years' imprisonment. Midway through her sentence, she participated in a restorative justice conference with the victim, who publicly praised the process.[644]

1016. **Restorative solutions case study (2023)** – A woman defrauded by her partner received answers, apologies, and emotional closure through a restorative justice process facilitated in prison. She credited the process with rebuilding her confidence and wellbeing.[645]

1017. These are only a small number of cases, but they do suggest that restorative justice can be adapted to fraud and can be appropriate where the offender is identifiable and victims are willing to engage. The willingness of the victim to participate in the process is key.

Conclusion

1018. This Review finds that, while empirical research on the effectiveness of restorative justice in fraud cases remains very limited, there is no principled barrier to its application. The UK framework is permissive in scope, allowing its use for any crime type, provided that both victim and offender give informed consent. This emphasis on inclusivity and stakeholder engagement aligns with the broader aims of rehabilitation and victim-centred justice.

1019. I do not wish to be misunderstood as recommending that all fraud cases should proceed by way of restorative justice. Clearly there will be cases where the offender is not identifiable, or the number of victims is too great. But there are sufficient signs that the Government should consider piloting a restorative justice scheme specifically for fraud cases, with a particular focus on low-level offending.

1020. Such a pilot could build on the 2017 trial conducted by the City of London Police and the Home Office, which demonstrated cautious optimism regarding behavioural change and victim engagement. While it is recognised that diversionary schemes may attract criticism for being perceived as lenient, restorative justice is not a substitute for prosecution. In

---

643 Gill, M. and Howell, C., *An evaluation of a restorative justice trial: where the victims are businesses and the offenders are insurance fraudsters*, report for the City of London Police, (2017).

644 Sussex Police and Crime Commissioner, 'Fraud victim praises restorative justice During International Restorative Justice Week', news story, 23 November 2017.

645 Restorative Cleveland, *Fraud Case Study: Prison-Based Restorative Justice Outcomes*, (2023).

some cases, it could be a viable alternative, but it can also be a complementary process that promotes accountability and recovery.

1021. I also note with concern that the latest data estimates that only 5.5% of victims with a known offender recalled being informed about restorative justice,[646] despite a clear entitlement under the Victims' Code. The Government should examine the extent to which police forces are meeting their obligations to inform victims of restorative justice options, particularly in fraud cases.

1022. At a minimum, the Review reiterates that this right is undiminished in fraud matters. There should also be consideration of how enforcement authorities assess whether a case is appropriate for restorative justice. It may be that, at an early stage, a case is seen as unsuitable, which would explain why only a small proportion of victims recall being informed of the process. It should be made clear that restorative justice can be used for all crimes, including fraud, and the assessment of suitability should follow clear and widely understood criteria.

1023. Restorative justice should no longer be treated as an 'optional extra'. It is a principled, structured, and potentially transformative tool that deserves a central place in the justice response to fraud.

Recommendation 42

Pilot a restorative justice programme for fraud cases, to be used only where it is assessed as appropriate and pursuant to clear criteria, and where both the offender and the victim provide informed consent. The scheme should facilitate structured dialogue aimed at acknowledging harm, promoting accountability and supporting victim recovery, and can operate alongside or as an alternative, to criminal proceedings.

[646] Office for National Statistics, *Restorative justice, year ending March 2011 to year ending March 2020: Crime Survey for England and Wales (CSEW)*, (2021).

19. Victims

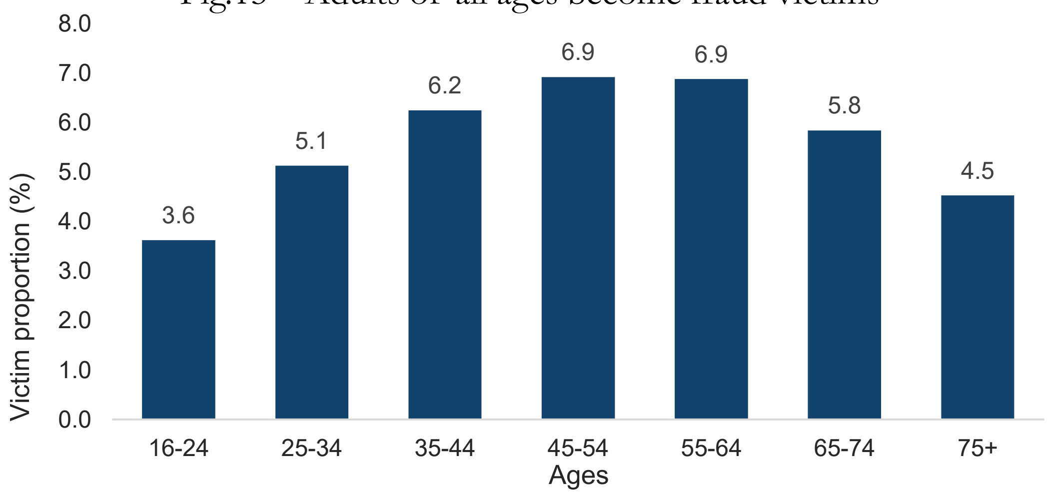
1024. As outlined at the beginning of this report, fraud has long occupied an uneasy position within the criminal justice system.[647] Historically, governments and courts have been reluctant to treat fraudulent conduct with the seriousness we have come to understand it deserves, debating not only whether certain behaviours should constitute criminal offences, but also whether they should be considered wrongful at all, rather than the result of sharp business practice. This narrative, which has persisted for decades and arguably until the turn of the decade, has contributed to the enduring myth that fraud is a victimless crime.

1025. Sustaining this view is a lingering societal attitude that victims of fraud are somehow complicit in their own misfortune. Such an interpretation is not only unjust, it is misleading, and the data tells a different story. Anyone can become a victim, including those we might least expect. It affects the vulnerable, yes—but also the financially literate, and those who believe themselves immune to deception. It is precisely this hubris that blinds us to the true nature of fraud: a pernicious crime, rooted in manipulation. It is not weakness that makes someone a victim of fraud, it is the human instinct to trust.

<u>Individuals</u>

1026. The notion that criminals target only the elderly or the uninformed is not borne out by the evidence. On the contrary, the data reveals that those most frequently victimised are adults in mid-life, specifically those aged 45–64, where prevalence reaches an estimated 6.9% of the cohort (see figure 15).[648] These are individuals often at the height of their careers and financial responsibilities.

Fig.15 – Adults of all ages become fraud victims

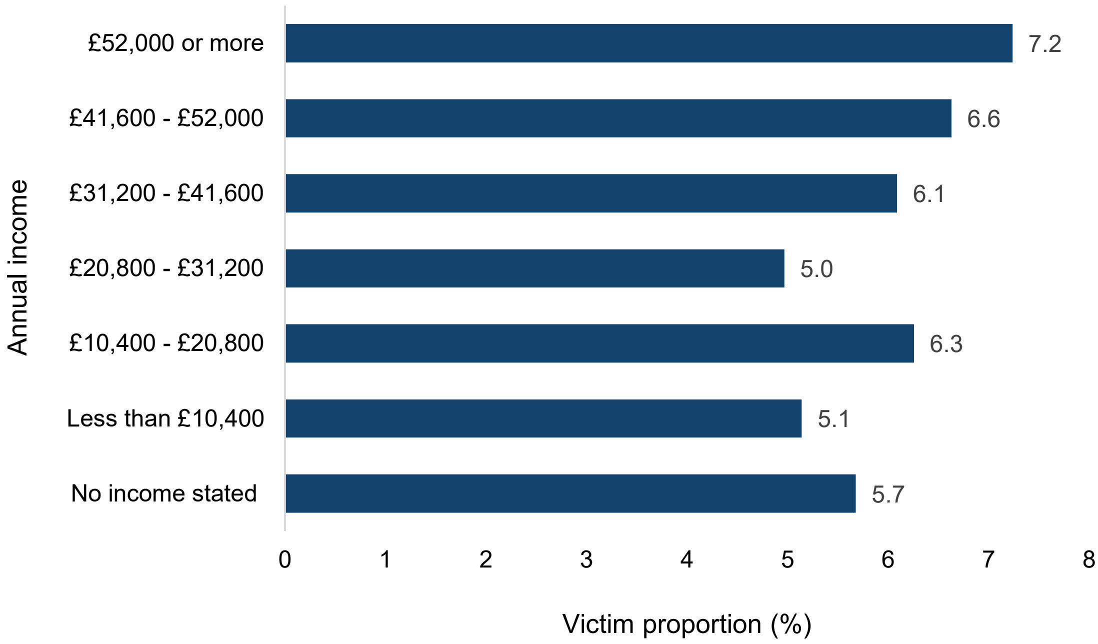


[647] See chapter 'A Short History of Fraud'.

[648] Office for National Statistics, *Nature of fraud and computer misuse in England and Wales*, appendix tables 7 and 8, year to March 2024. Does not include those under the age of 16.

1027. Income levels reveal a similar paradox. The highest earning households, those with incomes exceeding £52,000, are the most frequently targeted (7.2%), (see figure 16).[649] This is not accidental. Fraudsters seek out those with assets to lose.

Fig.16 – Higher earners at greater risk of fraud



1028. Occupational status further reinforces this pattern. Individuals in managerial or professional roles are disproportionately affected (6.8%), while those who have never worked or are long-term unemployed report the lowest victimisation rates (3.1%).[650] Again, this reflects the targeted and calculated approach of fraudsters.

1029. Tertiary education also offers no immunity. Those with degrees or diplomas are twice as likely to be victims (6.7%) compared with those with no formal qualifications (3.3%).[651] This is a reminder that academic achievement does not confer protection against deception.

1030. The figures above dispel society's expectations of the typical fraud victim. It is not true that those heavily targeted are among society's elderly or less educated, and it is certainly not true that the young and academically educated are immune. Risk-factors are wide-ranging, including individuals' disposition, an underestimation of personal risk, and market-based vulnerabilities.[652] Tertiary education, occupational status and high income have no correlation to reduced levels of fraud and, in some cases, perhaps align with an

649 Ibid.
650 Ibid.
651 Ibid.
652 Low, N. and Lally, C., *Social and phycological implications of Fraud*, UK Parliament Post, (2024), page 8.

increased chance of victimisation. It may be that those with the most to lose are often a fraudster's prime target.

Personal Impact

1031. The impacts on an individual, when they become a victim of fraud, vary in type and severity. Broadly, these can be delineated into financial and non-financial harms. Under the definition of fraud, set out in the Fraud Act 2006,[653] an attempt to make a gain or cause of loss of monies or assets is the central common denominator of every fraud. Any additional emotional or psychological harm inflicted therefore depends on the methodology of the specific fraud type and the circumstances of the victim.

1032. The financial consequences of fraud are as diverse as they are devastating. For some, the loss may be limited to modest sums, a few hundred pounds siphoned through an authorised pushed payment or phishing scam. For others, the impact is ruinous: house deposits, pension pots and life savings stolen in moments. Action Fraud data reveals that pension-related scams alone resulted in average losses of over £33,000 per victim in 2024, with total losses exceeding £17 million. These are not abstract figures, they represent the dismantling of futures and the theft of dignity. In the year to June 2025, victims of fraud incurred a financial loss in 74% of incidents.[654]

1033. As discussed, depending on the fraud methodology, some individuals may be covered by the mandatory reimbursement scheme, which currently covers incidents of authorised push payment (APP) fraud by up to £85,000.[655] This is not, however, a catch-all, with victims deemed to have committed 'gross negligence', and those impacted by other fraud types, left outside of this safety net.[656]

1034. Yet the true cost of fraud cannot be measured in pounds and pence alone. The emotional and psychological toll is substantial. A recent Home Office study found that 86% of fraud victims experienced anger, 73% stress, and 63% anxiety following their victimisation. Nearly one in five reported depression, and a small but significant number disclosed resultant suicidal thoughts or self-harm. Moreover, the analysis concluded that "the amount of money lost did not always correlate with the extent of wider harms experienced". These are direct consequences of the violation fraud represents, a breach not only of financial trust, but of personal autonomy.[657]

1035. Trust, once broken, is not easily restored. Nearly half of surveyed victims reported a diminished trust in others, and almost a third became reluctant to use the internet, a

---

653 See chapter 'Legislative Landscape'.

654 Office for National Statistics, *Statistics on Crime in England and Wales*, (2025), Estimated fraud incidents, year ending June 2025, appendix table C1.

655 Payment Systems Regulator, 'APP fraud reimbursement protections', (2024).

656 See chapter 'Corporate Responsibility'.

657 Home Office, *Experiences of victims of fraud and cyber crime*, (2025).

chilling outcome in an increasingly digital society. Victims spoke of feeling foolish, ashamed and isolated, particularly those who considered themselves financially literate or tech-savvy.[658] The stigma surrounding fraud, and the perception that one ought to have 'known better' compound the harm and deters reporting.

1036. In some cases, the damage extends beyond the individual to their relationships and sense of civic trust. Victims of romance fraud, for instance, described the collapse of friendships and the erosion of their ability to trust others. Others reported a loss of faith in institutions, banks, police and the State, particularly when support was slow, impersonal or absent.[659] The process of reporting fraud, when poorly handled, can itself become a secondary distress, forcing victims to relive their experience without assurance of redress.

1037. It is therefore imperative that fraud be recognised not merely as a financial offence. The impact on victims is multifaceted—economic, emotional, psychological and social.[660] Any meaningful response must reflect this complexity. Support services must be timely, empathetic and tailored.[661] Reimbursement schemes, while essential, cannot be the sole remedy.

Case Study – Dr Jonathan Leakey

Dr Jonathan Leakey, a 58-year-old retired university lecturer from Ballymena, became a victim of a sophisticated banking scam that cost him £25,000. The fraud began with a text message that appeared to come from his bank, warning of suspicious activity on his debit card. The message was inserted into a legitimate text thread from the bank, lending it credibility. Upon calling the number provided, Dr Leakey unknowingly disclosed sensitive information to fraudsters who then emptied his account. The psychological impact was severe, leaving him traumatised and anxious about using the internet. Following a nine-month campaign, Dr Leakey's bank refunded his loss.[662]

Businesses

1038. It is a common misconception that fraud is a crime whose victims are confined to individuals. In truth, businesses, large and small, are frequently the targets of fraudulent conduct, and the consequences for them can also be profound. The impact reverberates through the organisation's operations, its workforce and the wider economy. Recent analysis found that one in four businesses with employees experience fraud each year.[663]

---

658 Ibid.
659 Whitworth, D., 'Fraud victim's 18-month fight for £80,000 refund', BBC News, 8 May 2024.
660 Home Office, *Experiences of victims of fraud and cyber crime*, (2025).
661 See Recommendation 8.
662 Peachey, K., 'Fraud victim: "I got the shakes every time I went online"', BBC News, 15 October 2020.
663 Home Office and Ipsos, *Economic Crime Survey 2024*, (published November 2025), paragraph 2.1.

1039. At the systemic level, fraud can erode a business's liquidity, impairing its ability to meet short-term obligations. For enterprises operating on narrow margins, such disruption can be fatal. A single significant fraud event may precipitate a cash-flow crisis, forcing the business to curtail investment, defer payments to suppliers, or seek emergency financing at punitive rates. In extreme cases, otherwise viable businesses have been driven into insolvency, not as a result of an unsound model, but because fraud stripped them of the working capital essential to survival.

1040. Business victimisation impacts spread into the wider economy. When funds are diverted or lost, businesses often respond by reducing expenditure on recruitment, training and innovation. This contraction has a chilling effect on job creation and economic dynamism. The cumulative effect of such retrenchment, when replicated across sectors, is to depress employment opportunities and stifle growth.[664] Fraud, therefore, is not a victimless crime; it is a drag on productivity and a brake on economic progress.

1041. Finally, the collapse of a business due to fraud can have cascading effects on its stakeholders, employees, suppliers, customers and creditors. Supply chains are disrupted; contractual obligations go unmet; and confidence in the market is undermined. In aggregate, these failures erode trust in commercial dealings, increase the cost of doing business and necessitate higher levels of regulatory oversight. The economic harm, therefore, is not confined to the immediate victim but radiates outward, imposing costs on society at large.

Case Study – Kent Brushes

In 2023, Kent Brushes, a Hertfordshire-based manufacturer with an annual turnover of approximately £11 million, suffered a loss of £1.6 million following an APP fraud. The funds were stolen in under 20 minutes after a financial controller was manipulated into granting access to the company's bank account. The incident forced the business to slow the rollout of new products to maintain liquidity, although all staff salaries were met and operations continued. At the time of reporting, the business's bank declined reimbursement, citing the absence of consumer protections for business accounts.[665]

Reputation

1042. Fraud does not only deplete financial resources; it corrodes trust. For businesses, particularly those in financial services, the perception of weak fraud controls can damage client confidence and attract regulatory scrutiny. Regulators expect firms to maintain robust systems to prevent and respond to fraud; failure to do so risks sanctions, fines, and

664 RSM UK, 'Fraud loss reaches £2.3bn as fraudsters become increasingly sophisticated', news story, 28 April 2025.
665 Whitworth, D., '"My business had £1.6m stolen in 20 minutes"', BBC News, 22 October 2023.

intrusive oversight. The reputational harm from such failures often exceeds the immediate financial loss.

1043. It is also notable that some firms have historically preferred to absorb fraud losses quietly rather than pursue legal remedies or disclosure, fearing reputational damage. This instinct to conceal, however, carries grave risks: it emboldens fraudsters and, when exposed, can inflict greater harm on customer trust than the original offence.[666] Transparency and accountability are therefore essential to preserving market integrity and sustaining confidence in the financial system.

Current Services

1044. Once an individual or business has become a victim of fraud, the immediate question is not only how to recover losses, but how to access meaningful support outside of the traditional criminal justice process. The landscape of victim services in the United Kingdom is broad, but historically fragmented. While prevention remains a critical endeavour, I presently focus on the services available to those who have already suffered harm.

1045. Until December 2025, the State's primary support service was offered through the National Economic Crime Victim Care Unit (NECVCU), which was associated with Action Fraud and overseen by the City of London Police. NECVCU was established in 2018 to address the inherent limitation of a centralised and often faceless reporting portal. The unit's aim was to provide tailored support to fraud victims, especially those deemed vulnerable, through trained advocates who offer reassurance, guidance and practical advice.

1046. A 2025 Home Office study found that victims who received NECVCU support reported significantly higher levels of satisfaction and emotional recovery than those who did not.[667] The unit's expansion, in 2023, to all 43 police forces in England and Wales marks a significant step forward, but demand continues to outstrip capacity.[668]

1047. Since the replacement of Action Fraud with the new service Report Fraud,[669] NECVCU has been replaced with the Report Fraud Victim Services.

---

[666] Dunkley, E., 'Lloyds to review all customers affected by HBOS scandal', *Financial Times*, 7 February 2017.
[667] Home Office, *Experiences of victims of fraud and cyber crime*, (2025).
[668] City of London Police, 'Specialist victim care unit which supports thousands of vulnerable fraud victims rolled out across the UK', press release, 3 August 2023.
[669] City of London Police, *Report Fraud*, [Accessed 8 December 2025].

Case study – NECVCU's Impact

While it has not existed in its current format for a significant period of time, NECVCU, now Report Fraud Victim Services, has inarguably had a positive impact on the victim support system. In October 2025 alone, the service engaged 17,379 victims, bringing the total number of victims supported to 1,018,427 by the end of that month.

The unit reported significant financial savings too, recording that they have prevented frauds to the sum of almost £14 million and secured reimbursement for victims totalling over £6 million.[670]

1048. Financial redress is another critical component. The introduction of the mandatory reimbursement scheme in October 2024 has seen over 85% of money lost return to victims for APP fraud.[671] However, this success masks deeper concerns. Reimbursement does not prevent fraud, nor does it address non-financial harm, instead it shifts financial liability from victims to banks.

1049. Beyond law enforcement support services, a network of third-party organisations plays a vital role. Charities such as Victim Support[672] and Cifas[673] offer emotional counselling, fraud prevention advice and identity protection services. Victim Support, in particular, provides 24/7 helplines and one-to-one support, helping victims rebuild trust and navigate complex recovery processes. Cifas offers protective registration to shield individuals from identity theft and works with local authorities to safeguard vulnerable adults.

Evaluation

1050. There is no shortage of organisations committed to supporting victims of fraud. From statutory bodies such as NECVCU, to charities like Victim Support and Cifas, the infrastructure is broad and, in many cases, becoming increasingly effective. These services offer practical guidance, emotional support and identity protection, often bridging the gap left by overstretched law enforcement.

---

670 Information provided by the City of London Police. The service estimated to have saved £13,972,168 being lost to fraud since January 2021, helping victims recover £6,165,845.
671 Payment Systems Regulator, *The story so far: A snapshot of what we've seen since our APP scams reimbursement requirement went live*, (2025).
672 Victim Support.
673 Cifas.

1051. However, the sheer number of fraud victims in England and Wales presents a formidable obstacle, reaching into the hundreds of thousands, if not millions.[674]

1052. Although it is currently thought that only 13% of all frauds are reported,[675] the question remains as to how the State should provide meaningful and effective support to such a significant number of individuals and businesses, particularly noting that those who do not report are left invisible to the system.

1053. This Review heard that media portrayals of fraud victims often reinforce harmful stigma, depicting them as gullible, careless or complicit. This narrative discourages reporting and fosters shame. Secondly, there is no dedicated support pathway for victims under 18, despite rising levels of youth-targeted scams, particularly via social media and gaming platforms. Young people are increasingly exposed to fraud, yet services remain adult-centric and reactive.[676]

Victim Access to Proceeds of Crime Act 2002 Proceedings

1054. Beyond its enforcement utility, the Proceeds of Crime Act 2002 (POCA) offers a vital but underused avenue for victim redress. Where the return of lost funds provides meaningful compensation, POCA can help victims feel that justice has been done—even as criminal proceedings move slowly. Yet, despite Section 10A granting victims a statutory right to make representations in confiscation proceedings, this right is rarely exercised, largely because victims are unaware of it. There is a clear opportunity to make better use of these provisions, particularly where assets have been frozen. Victims should therefore be proactively informed of their entitlement to participate in proceedings whenever they have a legitimate interest in the outcome.

1055. One such solution would be to capitalise on changes made through the Victims and Prisoners Act 2024,[677] which strengthened the statutory framework for victim rights. The Act clarifies that economic harm[678], including financial loss from fraud, constitutes victimisation. The Act also places the Victims' Code[679] on a legal footing, requiring criminal justice agencies to keep victims informed, provide access to support services and collaborate across sectors. As the definitive resource, this would be a fitting vehicle to communicate to fraud victims regarding their ability to participate in POCA proceedings.

---

674 See chapter 'Contemporary Picture'. Office for National Statistics, *Statistics on Crime in England and Wales* (2025), (T)CSEW estimated fraud incidents, year to June 2025.
675 Ibid.
676 Crest Advisory, *Understanding and Addressing Fraud Against Children and Young People: An Action Plan*, (2024), [Accessed 10 October 2025].
677 Victims and Prisoners Act 2024.
678 Ibid, c. 21, Part 1, s.1(a).
679 Ministry of Justice, *Code of Practice for Victims of Crime in England and Wales*, (2020).

Recommendation 43

Victims of fraud should be clearly informed, through an amendment to the Victims' Code, of their right to participate as third parties in Proceeds of Crime Act 2002 proceedings, particularly where law enforcement agencies have frozen assets linked to criminal conduct.

Conclusion

1056. Victims must not be relegated to the margins of the Government's response to fraud. While criminal court backlogs are delaying justice, this must not mean that access to support is also slow. As the Government works to improve case progression, it must ensure victims are kept informed and engaged throughout the process, so they do not feel neglected or excluded from justice (see Recommendation 8).

1057. The State has a clear duty to ensure that those who suffer loss, whether individuals or businesses, are not left adrift while the criminal process grinds on. Restoring dignity and autonomy is not an optional extra; it is fundamental to public confidence. This requires a system that is visible, accessible and properly resourced. Anything less risks compounding the original harm and eroding trust in the very institutions charged with protection.

1058. The Government's new strategy[680] should recognise victims as central stakeholders, not passive observers. This means embedding victim rights within legislative frameworks, ensuring consistent application of the Victims' Code, and leveraging mechanisms such as POCA to deliver tangible outcomes.

1059. Ultimately, success should not be measured solely by conviction rates but by the restoration of confidence—confidence that the State values those harmed, acts swiftly to mitigate loss, and provides clear pathways to recovery while fundamentally improving the criminal justice response.

[680] Home Office, 'Lord Hanson unveils ambitious new approach to tackling fraud', news story, 27 March 2025.

20. Education and Awareness

1060. While an effective criminal justice response is essential to securing justice for victims of fraud, equal emphasis must be placed on prevention. Protecting individuals and businesses from becoming victims requires proactive measures, particularly through awareness and education. Although an in-depth evaluation of fraud education policies falls outside the scope of this Review, it is important to recognise their significance. In recent years, the Government and its partners have made meaningful progress in prioritising fraud prevention messaging.

'Stop! Think Fraud'

1061. The 2023 Government Fraud Strategy committed to modernising public anti-fraud communications through a unified, cross-system campaign.[681] In collaboration with the National Cyber Security Centre, City of London Police and the National Crime Agency, the Home Office subsequently created 'Stop! Think Fraud', which launched in early 2024.[682] The ongoing campaign focuses on educating the public about the risks of fraud and emphasises that anyone can become a victim. It secured broad support across the technology, financial and legal sectors, as well as victim agencies and consumer groups, leveraging email alerts, banking notifications and social media channels, though no data has been published on its efficacy.

1062. While the campaign has been effective, it would benefit from more precise targeting of high-risk regions and demographics. Action Fraud data indicates that the proportion of adults reporting fraud victimisation varies significantly across English regions: South West (7.8%), South East (7.0%), and East Midlands (6.4%) compared with the North East (4.2%).[683] This disparity merits further analysis but demonstrates that fraud is not evenly distributed across the country.

1063. Disability status is another critical vulnerability. Adults with disabilities are markedly more likely to be victims (7.5%) than those without (5.3%).[684] These figures, together with those highlighted in the preceding chapter, demand attention. They underscore the imperative for targeted education initiatives that reach those most at risk—dispelling the persistent misconception that vulnerability to fraud is confined to the elderly.

1064. A centralised campaign such as 'Stop! Think Fraud' is valuable but could have greater impact if messaging was adapted to specific regions and demographics. Future strategy should combine national reach with local precision, ensuring resources are directed where

---

[681] Home Office, *Fraud Strategy: stopping scams and protecting the public*, (2023), CP 839, page 38.
[682] 'Stop! Think Fraud', Gov.UK Campaign, [Accessed 8 December 2025].
[683] Office for National Statistics, *Nature of fraud and computer misuse in England and Wales: appendix tables*, (2024), Table 8.
[684] Ibid.

risk is highest. There is also an opportunity for local law enforcement officers to assist in reaching those individuals who may be digitally excluded or more at risk of fraud. Ensuring that vulnerable groups receive more personal and tailored education will help prevent victimisation.

Recommendation 44

Enhance and target the 'Stop! Think Fraud' public awareness campaign to better protect high-risk regions and vulnerable demographics.

Financial Education

1065. Effective fraud prevention cannot be separated from education, and there is no shortage in financial education resources that help learners better equip themselves to spot and avoid fraud. These include resources developed in partnership with the Home Office and the National Crime Agency which have been made available to schools, including lesson plans and online workshops delivered by the Association for Citizenship Teaching.[685] The material incorporates case studies, practical guidance on identifying fraudulent behaviour, and advice on avoiding money mule recruitment. Cifas has also produced anti-fraud lesson plans targeted at Key Stage 3 and 4 pupils, focusing on protecting personal information online and critically assessing digital content.[686]

1066. Private sector institutions such as consumer banks, including NatWest,[687] also offer fraud education for customers through programmes such as MoneySense and Financial Foundations, alongside webinars. Businesses can access learning through the National Cyber Protect Network, led by the City of London Police, which supports organisations in defending against cybercrime and fraud. Beyond these, numerous programmes seek to upskill individuals and enterprises, yet the central challenge lies not in the availability of training, but in its practical impact. Two issues arise.

1067. First, a technique frequently deployed in authorised push payment fraud is the deliberate imposition of urgency. Fraudsters create an illusion of time pressure so compelling that it overrides the victim's capacity for slow, critical thought, the very process that might otherwise trigger recall of prior fraud-prevention training. This reality underscores education as a vital pillar of prevention, but emphatically not a panacea.

1068. The second challenge is ensuring that high-quality training and anti-fraud resources, whether online or in hard copy, reach those most at risk and are delivered in a manner

[685] Association for Citizenship Teaching, *Fraud Education - in collaboration with the Home Office and the National Crime Agency*, [Accessed 12 November 2025].
[686] Cifas, 'Anti-Fraud Lesson Plans', [Accessed 5 December 2025].
[687] NatWest, 'Start your fraud learning',[Accessed 12 November 2025].

that secures comprehension and retention. The task is to bridge the gap between resource and recipient, and to do so in a way that confers the greatest practical protection.

1069. Further, this Review heard concerns that fraud education within schools occupies a narrow space in the curriculum, constrained by funding and time pressures. To mitigate these challenges, the following recommendations aim to address gaps in provision and strengthen outcomes, measures which, in turn, will help reduce fraud.

Recommendation 45

Fraud prevention and ethical awareness should be more explicitly embedded in the national curriculum. While some elements exist within personal, social, health and economic (PSHE) education, this foundation should be strengthened by integrating structured content on fraud risks, dishonesty and ethical decision-making—particularly in digital and financial contexts. This should be delivered through modules on internet safety, digital literacy, or citizenship, with a focus on real-world scenarios such as online fraud and money muling.

1070. Alongside compulsory education in schools, there is scope for targeted intervention at a critical juncture: the opening of a bank account. For many young people, this step towards financial autonomy occurs as early as the age of 16,[688] where bank accounts can be opened without parental consent. It is a moment of opportunity, but also vulnerability.

1071. Unlike regulated products that carry mandatory health and safety warnings, access to banking brings exposure to high-speed payments, international transfers and digital platforms yet rarely comes with clear guidance on the attendant risks. This gap is significant. Without concise, compelling education at the point of account opening, young people remain susceptible to fraud, money muling and other forms of exploitation. The case for intervention is clear: prevention must begin where financial independence begins.

1072. The Financial Conduct Authority should require banks to take responsibility for educating customers who are under 18 years old about the risks associated with opening a bank account. Where an account can be opened by a child without parental consent, banks should deliver a clear and engaging briefing, rather than a formal educational programme, before activation. This briefing should explain that financial independence brings exposure to serious risks and legal obligations. It could take the form of a concise video or interactive module, accessible via mobile application, and should cover:

a. **Fraud** – The key warning signs and common methods used by criminals.

b. **Money muling** – Its illegality and the potential criminal consequences.

[688] The Cooperative Bank, '[Bank accounts for 16 and 17 year olds](https://)', [Accessed 8 December 2025].

c. Practical indicators of suspicious activity and steps to stay safe.

1073. Such an approach would make warnings harder to ignore by presenting them in a format that is accessible and compelling. It would also help ensure that vulnerable individuals understand how to avoid victimisation. The objective is to promote early financial awareness and reduce exploitation of young people in criminal schemes, complementing school-based education and closing gaps in protection.

Recommendation 46

The Financial Conduct Authority should work with consumer banks to introduce mandatory educational learning for individuals under 18 years old before they can open an account. This could take the form of a short video or interactive session delivered via a mobile application, which explains the risks of fraud, scams and money muling. The goal is to promote early financial literacy and reduce the risk of exploitation of young people in facilitating fraud and money laundering.

1074. Education alone will not eliminate fraud, but it is a vital piece of the puzzle. When combined with a stronger criminal justice response, it helps build a society that is resilient, harder for criminals to target and exploit. Awareness equips individuals and businesses to recognise risks early, reducing opportunities for harm. Alongside enforcement and prevention measures, education fosters a culture of vigilance and shared responsibility, ensuring that fraud becomes more difficult to perpetrate and less likely to succeed.

21. Conclusion

1075. Fraud is no longer a peripheral irritant, but a systemic risk to personal autonomy, national prosperity and public trust. The policy centre of gravity has rightly begun to move upstream. At home, mandatory reimbursement for authorised push payment victims is reshaping incentives across the payments chain; online platforms now face duties, backed by Ofcom, to assess illegal-content risks, remove fraudulent advertising and design safer systems. Abroad, partners are adopting a similar posture: the United Kingdom (UK) has supported a second Global Fraud Summit convened by the UN Office on Drugs and Crime (UNODC) and the International Criminal Police Organization (Interpol) to drive coordinated disruption and large-scale intelligence sharing—an explicit commitment that the fight against fraud must be international in method as well as in ambition.

1076. Success will turn not on the elegance of any single statute but on delivery discipline and cross-sector accountability. That requires purposeful public–private collaboration grounded in law, with clear, codified gateways for two-way data exchange and transparent guardrails. The international trend points the same way: partnerships must be designed for results, not merely convened for appearances.

1077. Accordingly, the final proposal in this Review is intentionally structural. Recommendation 47 sets the governance spine that stitches together the reforms in these pages, placing fraud on a whole-system footing with clear mandates, shared metrics and public accountability across law enforcement, regulators, technology and telecoms, payments, and the courts. Its purpose is practical: to make deterrence credible, disruption routine and victim progress visible and to ensure that platforms and payment firms carry a fair share of responsibility.

1078. This spine should be led by visible ministerial authority. The Government's elevation of fraud to full ministerial status, Lord Hanson's portfolio and public commitments to accelerate data-sharing, strengthen international cooperation and deliver a refreshed national strategy, signals the right direction of travel. It is a foundation on which to embed a single system owner who can set targets, chair a strengthened Joint Fraud Taskforce, publish an annual scorecard, and hold departments, regulators and industry to outcomes rather than intentions.

Recommendation 47

Appoint a cross-Government Fraud Lead ('Fraud Czar') to drive strategic coordination and accountability in the United Kingdom's response to fraud. This senior figure should be empowered to lead the Government's fraud agenda across departments, ensuring coherence between emerging threats, policy, enforcement, prevention, and victim support.

1079. The UK has begun to treat fraud as a defining crime of the digital age. The task now is to turn intent into sustained delivery—lawful data-sharing at speed, consistent corporate accountability, targeted powers at the margins, international reach, and visible leadership that makes the whole system answer for outcomes. The measures put forward this Review should shift the dial, to ensure that the time when there has been little to deter fraudsters is over. This is not only a matter of maintaining law and order; it is a duty to secure justice for the more than four million adults who fall victim to fraud each year.

22. List of Recommendations

1. Grant law enforcement the power to issue civil fines to individuals purchasing fraud-enabling products online, drawing on provisions in the Public Authorities (Fraud, Error and Recovery) Act 2025 [Chapter 5]. Law enforcement should also retain discretion to pursue prosecution and custodial sentences in serious cases.

2. Introduce a new corporate criminal offence for providers of regulated user-to-user services (as defined under the Online Safety Act 2023) who fail to prevent fraud on their platforms. This offence would closely mirror the recently introduced 'failure-to-prevent' fraud offence under the Economic Crime and Corporate Transparency Act 2023, which holds large organisations criminally liable if they fail to prevent fraud committed by associated persons for their benefit.

3. Introduce an anti-fraud levy on digital and communications infrastructure providers, including social media platforms, online service providers, and other intermediaries that host or facilitate fraudulent activity. The levy would aim to distribute the financial burden of economic crime more equitably across all stakeholders whose platforms are exploited for fraud. It would be administered by Ofcom, with a sunset clause allowing for its reduction or removal if measurable improvements in fraud prevention, detection, and cooperation with law enforcement are demonstrated.

4. Introduce a specific summary-only offence of identity-based impersonation, defined as the use of another person's personal details or identity for the purpose of committing fraud.

5. Create a summary-only offence for Deed Poll Abuse—changing one's name through the deed poll process with the intent to commit a fraud.

6. An adaptable approach should be adopted to tackle low-level money laundering:

    a. Depending on the severity of the offence, law enforcement should be granted discretion to either issue a formal warning (Cease and Desist Notice) to first-time offenders, refer culprits to mandatory re-education programme, or pursue prosecution if appropriate.

    b. Where offending continues, law enforcement should have the option to impose a civil penalty, such as a fixed penalty notice.

    c. Where offending further continues or is substantial in the first instance, law enforcement should consider prosecution under the new proposed summary-only money laundering offence, the Proceeds of Crime Act 2002 or other relevant legislation.

a. Guidance should be issued, by the National Police Chiefs' Council and Crown Prosecution Service, to help law enforcement identify vulnerable individuals, including those who may have been coerced into offending.

7. Create a summary-only offence for low-level money laundering—allowing a bank account to be used directly or indirectly by another person without a reasonable excuse.

8. Report Fraud should publicly commit to a 14-day service standard, ensuring that every victim receives a clear update on the status of their report within that timeframe. This commitment should cover three key elements:

   a. Acknowledgement and Case Reference – Immediate confirmation of the report with a unique reference number.

   b. Triage Decision – Completion of an initial assessment and prioritisation within 14 days, with the outcome communicated to the victim.

   c. Accessible Progress Tracking – Provision of a secure, user-friendly platform enabling victims to monitor progress, view updates, and access support resources at any time.

9. Intelligence sharing within public–private partnerships focused on tackling economic crime should take place within a statutory framework.

10. UK law enforcement agencies should collaborate with the private legal sector market in a fair, transparent and open manner, to facilitate the recovery of losses sustained by a victim of fraud.

11. Until a statutory framework has been created, establish a single memorandum of understanding between public bodies setting out how data and intelligence can be shared between these agencies, for the purpose of detecting and investigating fraud.

12.

   a. The Home Office, working with the National Crime Agency (NCA) and Information Commissioner's Office, should provide guidance on voluntary and compelled data-sharing for public and private sector organisations, drawing upon section 7 of the Crime and Courts Act 2013, regulation 103(1) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017, and the Economic Crime and Corporate Transparency Act 2023. This should explicitly cover information sharing between private sector organisations, setting out the legal basis and safeguards.

   b. The Government should clarify the scope of sections 333 and 342 of the Proceeds of Crime Act 2002 concerning the tipping off offence and the prejudicing of an investigation. The NCA should provide assurance that, where information is shared with the objective being to combat criminal activity in line with this guidance these provisions will not apply.

13. Section 3 of the Criminal Justice Act 1987 should be amended to mirror the information gateway in Section 7 of the Crime and Courts Act 2013, thereby enabling the Serious Fraud Office to share and receive information with greater flexibility and operational reach.

14. The Government to conduct a comprehensive review of the data-sharing provisions and arrangements to enable the detection and investigation of fraud. This should include sharing within and between the public and private sectors.

15. Make legislative provision for the Serious Fraud Office to financially reward whistleblowers. The Government should launch a consultation to inform the design of a suitable scheme.

16. Create a new criminal offence for individuals who knowingly make false reports to the law enforcement agencies under a whistleblower incentivisation scheme. The person is not in breach of this offence if he does not know or suspect the report or evidence submitted to be false.

17. Establish a criminal offence for those who harass or intimidate whistleblowers.

18. Establish an independent arbitration panel to review appeals or complaints made by whistleblowers.

19. Funding should be prioritised to support the implementation of artificial intelligence by law enforcement agencies in the proactive detection and disruption of fraud.

20. The Law Commission recommendation 8, from its report *Search Warrants* (2020), should be implemented.

    Namely that the Insolvency Service be empowered to execute search warrants obtained under the Police and Criminal Evidence Act 1984 (Department of Trade and Industry Investigations) Order 2002, without the need to accompany a constable. This would extend to exercising the powers of entry as well as search.

    That sections 19 to 22 of the Police and Criminal Evidence Act 1984 be extended to the Insolvency Service, with necessary modifications.

21. The extraterritorial ambit of section 2(3) of the Criminal Justice Act 1987 should be reviewed with a view in particular to expanding jurisdiction to enable the Serious Fraud office to serve a notice on:

a. A United Kingdom (UK) person who is a director of a UK company and who is overseas.

b. A foreign corporate without a UK presence but a sufficient UK connection.

22. To prevent otherwise lawful section 49 Regulation of Investigatory Powers Act 2000 (RIPA) notices being frustrated because relevant data is stored remotely rather than locally, it is recommended the Act be amended as follows:

a. References to protected information having come into the 'possession' of a person should include protected information not stored locally on the device but accessible through a network connection.

b. Paragraph 1(1)(a) of Schedule 2 should be amended to permit appropriate permission to be given by a lay justice.

c. Section 53(5A)(a) should be amended so that the appropriate maximum term in a 'fraud case' is five years, adopting the same model for child indecency cases by providing a list of relevant fraud offences which engage the increased appropriate maximum term.

Search warrant application forms should be amended to:

a. Ask an applicant whether he or she intends to apply for appropriate permission to impose a disclosure requirement under section 49 of RIPA.

b. Guide the applicant through the relevant statutory test.

23. Establish a presumption in favour of use of the court's power under Section 41(7) of the Proceeds of Crime Act 2002 to make restraint orders in fraud cases, unless there is a compelling reason to oppose such an order.

24. The United Kingdom Government should take the lead in developing a protocol to the United Nations Convention against Cybercrime, ensuring fraud is recognised as a priority

25. Designate foreign nationals orchestrating transnational fraud for targeted sanctions. This measure would enable the United Kingdom (UK) to impose asset freezes, travel bans and other penalties on individuals based overseas who coordinate or profit from large-scale fraud operations targeting UK citizens.

26. Deny United Kingdom (UK) visas from foreign nationals linked to fraud against UK victims, in line with existing powers under the Immigration Rules and the Sanctions and Anti-Money Laundering Act 2018. This complements the Government's use of targeted immigration sanctions against individuals involved in transnational criminal activity.

27. Use trade agreements and memorandums of understanding to promote international law enforcement cooperation on evidence gathering, asset recovery, and extradition in fraud/economic crime cases affecting UK residents.

28. Invite the Judicial College to:

    a. Review how best to prepare all judges, including magistrates, for the likely increase in hearing cases relating to artificial intelligence-enabled fraud and the laundering of money/assets using cryptocurrencies.

    b. Review and update the existing 'Long and Complex Trials' course and to propose updating the training, or establish a bespoke module, covering the unique challenge of managing increasingly digital-heavy, serious and complex economic crime cases, and whether this training should be a requirement for all judges who hear complex economic crime.

29. Judges assigned to preside over a serious or complex economic-crime trial (including fraud) should be allocated within four weeks of the case being transferred to the Crown Court. The allocated judge should then be afforded a minimum of one week's uninterrupted reading time before arraignment, to enable effective case management and the early resolution of disclosure issues. This standard should be embedded in judicial scheduling as a matter of principle, to secure fairness, efficiency and public confidence.

30. The Judicial Office should extend the application of the Southwark Protocol to all Crown Courts across England and Wales that hear serious fraud and economic crime.

31. The Judicial Office should codify the Southwark Protocol into a Judicial Practice Direction to ensure consistent application across all Crown Courts.

32. Invest in modern court technology infrastructure across England and Wales to support the effective trial of complex fraud cases.

33. Extend civil powers already available to the Crown Courts, namely provisions under section 2 of the Company Directors Disqualification Act 1986, to enable courts to wind up a company explicitly being used, by a defendant, to commit fraud. Such powers would complement the introduction of a Criminal Receivership Order to strengthen the enforcement of financial penalties and asset recovery in economic crime cases (as proposed in Recommendation 3.9 of the Independent Sentencing Review).

34. Pilot 'diversion from court' schemes for low-level fraud offenders, particularly where there is early admission of responsibility.

35. Update the sentencing framework for serious fraud offences and money laundering, increasing the maximum custodial penalties to 20 years to reflect the gravity and impact

of these crimes. It is for the Sentencing Council to review these proposals and to consider guidelines for sentencing for the most serious offenders.

36. The Government should review and reform the current early guilty plea framework for complex fraud and economic crime cases. Specifically:

   a. **Enhanced judicial indications** – Replace the current approach with a reformed *Goodyear* indication process, enabling judges to provide a specific sentence indication (rather than a broad range) should an early guilty plea be considered. This would give defendants greater clarity and incentivise early resolution.

   b. **Increased sentence discount for very early pleas** – Introduce a 50% significant sentence reduction for guilty pleas entered at the earliest opportunity, reflecting the significant savings in time and cost for the justice system and the benefit to victims.

37. Introduce a statutory provision under Chapter 3 of the Sentencing Act 2020, mirroring section 74, which would enable discounted sentences where there is swift full payment of confiscation orders. This is in contrast to the current model of extending custodial sentences for delayed payment.

38. The Ministry of Justice should begin systematically collecting and publishing data on the number of individuals imprisoned for failing to satisfy a confiscation order. This dataset should include a breakdown by the value of the order, using the following bands:

   a. Less than £1 million.

   b. £1 million–£5 million.

   c. £5 million–£10 million.

   d. More than £10 million.

39. The Government should consider creating a separate statutory, court-supervised deferred prosecution mechanism for directors, senior managers and, where justified, other employees materially implicated in serious corporate economic crime. Any such mechanism should operate alongside, and not in place of, corporate liability, and should be capable of incorporating appropriate preventative measures, including restrictions akin to serious crime prevention order measures, where proportionate.

40. Proceeds of Deferred Prosecution Agreements should be injected into the criminal justice system and a proportion ring-fenced for economic crime enforcement activity.

41. The Government should legislate to create a fraud-specific civil protective order regime, modelled on Part 4 of the Policing and Crime Act 2009, empowering magistrates' courts to impose tailored restrictions on individuals suspected of minor fraud. This regime

should include financial, business and digital activity controls, alongside positive compliance requirements, and operate within a framework of judicial oversight and proportionality.

42. Pilot a restorative justice programme for fraud cases, to be used only where it is assessed as appropriate and pursuant to clear criteria, and where both the offender and the victim provide informed consent. The scheme should facilitate structured dialogue aimed at acknowledging harm, promoting accountability, and supporting victim recovery, and can operate alongside or as an alternative, to criminal proceedings.

43. Victims of fraud should be clearly informed, through an amendment to the Victims' Code, of their right to participate as third parties in Proceeds of Crime Act 2002 proceedings, particularly where law enforcement agencies have frozen assets linked to criminal conduct.

44. Enhance and target the 'Stop! Think Fraud' public awareness campaign to better protect high-risk regions and vulnerable demographics.

45. Fraud prevention and ethical awareness should be more explicitly embedded in the national curriculum. While some elements exist within personal, social, health and economic (PSHE) education, this foundation should be strengthened by integrating structured content on fraud risks, dishonesty, and ethical decision-making—particularly in digital and financial contexts. This should be delivered through modules on internet safety, digital literacy, or citizenship, with a focus on real-world scenarios such as online fraud and money muling.

46. The Financial Conduct Authority should work with consumer banks to introduce mandatory educational learning for individuals under 18 years old before they can open an account. This could take the form of a short video or interactive session delivered via a mobile application, which explains the risks of fraud, scams, and money muling. The goal is to promote early financial literacy and reduce the risk of exploitation of young people in facilitating fraud and money laundering.

47. Appoint a cross-Government Fraud Lead ('Fraud Czar') to drive strategic coordination and accountability in the United Kingdom's response to fraud. This senior figure should be empowered to lead the Government's fraud agenda across departments, ensuring coherence between emerging threats, policy, enforcement, prevention, and victim support.

23. Annex A – Terms of Reference

Independent Review of Disclosure and Fraud Offences – Part Two

Context

Following the delivery of the Report for Part One of the Independent Review *Disclosure in the Digital Age*, the Independent Review has commenced Part Two, an examination of fraud offences.

There has not been an independent review of fraud since 1986.[689] Since that time, the nature and scale of fraud has evolved considerably, now constituting over 40% of all surveyed offences in England and Wales.[690] As the proportion of online-enabled fraud has increased, so have the challenges facing investigators and prosecutors.

The impact on businesses, individuals and the wider economy has also risen. In the UK, an estimated £2.2 billion pounds was lost to fraud reported in the year ending November 2024. A likely underestimate, this figure does not fully reflect the serious emotional and psychological harm fraud can cause, with significant barriers remaining that prevent victims from receiving justice.

Scope

Part Two of the Review will examine the largest challenges faced by law enforcement in bringing criminals committing fraud offences to justice in England and Wales.[691]

It will consider key issues in each following stage of the fraud-life cycle:

a. **Reporting and disruption –** The means and methods by which law enforcement agencies can detect and disrupt fraudulent activities. This will include evaluating incentives for criminal fraud networks informants and whistleblowers.

b. **Investigation** – The skills, tools and powers required for investigators to rapidly pursue leads and share relevant data with private partners and other law enforcement agencies, including internationally.

c. **Prosecution and offences** – Evaluating whether fraud offences and the Fraud Act 2006 can keep pace with modern offending. Assessing enablers of fraud such ID theft, abuse of deed poll and the use of artificial intelligence. Considering whether there should be a greater role for civil penalties.

d. **Courts** – Assessing whether criminal courts are equipped to hear complex fraud cases.

e. **Penalties** – Whether the current penalties fit the crime. Looking beyond custodial sentences, the Review will consider if courts should be able to use more

---

689 The Roskill Report on Fraud Trials, HL Deb, vol. 469, (1986).

690 As of the year ending December 2022. Crime in England and Wales, *Appendix tables - Office for National Statistics*, Table A1

691 The Review will focus on England and Wales, and findings and recommendations will be shared with policymakers in Northern Ireland.

creative punitive measures. This will include evaluating penalties for companies failing in their duties to reduce and prevent fraud.

f. **Rehabilitation** – Consideration will be given to whether the current network of support for victims is sufficient and what more can be done to rehabilitate offenders.

Process

As the department responsible for tackling fraud against individuals and businesses, the Home Office will provide the Review secretariat, with policy support from the Attorney General's Office and the Ministry of Justice.

Outputs

The Review chair will report their findings and recommendations, which the Government will respond to in the usual way.

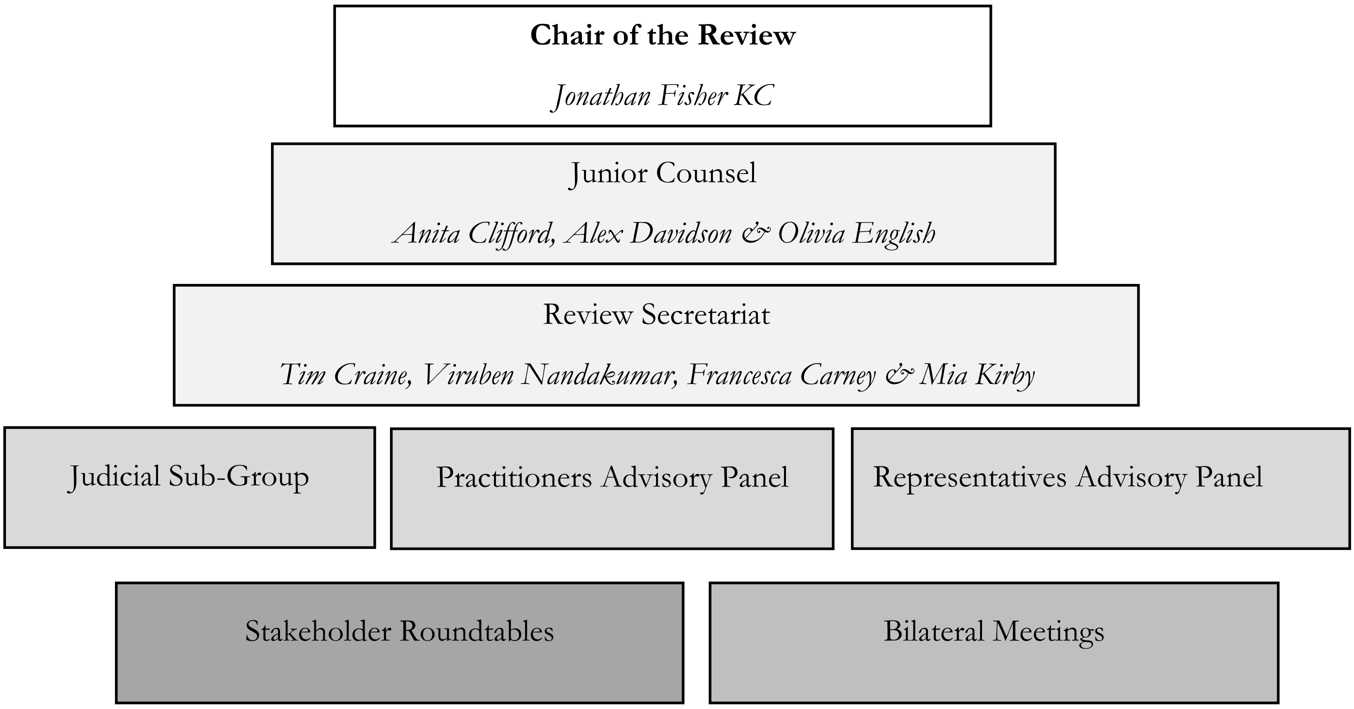
Timing

The delivery deadlines for each part of the Review have been revised to meet the following deadlines:

Part 1: Completed – November 2024.

Part 2: Fraud Offences Recommendations – Winter 2025/2026.

24. Annex B – Governance



25. Annex C – Summary of Engagement

Stakeholders

Academics

Bar Council

City of London Police

College of Policing

Consumer banks representatives

Criminal Bar Association

Crown Prosecution Service

Digital Police Service

Experienced defence practitioners

Financial Conduct Authority

HM Crown Prosecution Inspectorate Service

HM Revenue and Customs

Information Commissioner

Insolvency Service

Judicial Office

Judicial Sub-Group

Law Commission

Law Society

London Criminal Law Courts Solicitors' Association

Metropolitan Police

National Crime Agency

National Police Chiefs' Council

Ofcom

Independent Review of Criminal Courts

Independent Review of Sentencing

Independent Reviewer of Terrorist Legislation

Practitioners Advisory Panel

Private prosecutors

Regional Organised Crime Units

Representatives Advisory Panel

Royal United Services Institute

Serious Fraud Office

Southwark judges

Technology and social media companies

Tech UK

Telecommunications companies

UK Finance

Victims' Commissioner

Roundtables

Defending Session

Education & Prevention Session

Fraud Detection Session

Investigation Session

Offences & Penalties Session

Prosecution Session

Victim Support & Rehabilitation Session

Representatives Advisory Panel Membership

Amir Abid – Inspector, Gloucestershire Police

Nik Adams – Assistant Commissioner, City of London Police

Katy Barrow-Grint – Deputy Chief Constable, Gloucestershire Police

Graeme Bigger – Director, National Crime Agency

Tijs Broeke – Chair of the City of London Police Authority Board

Gary Cathcart – Head of Financial Investigation, National Crime Agency

Vincent Coughlin KC – Chief Criminal Counsel, Financial Conduct Authority

Jamie Daniels – Chief Superintendent, Criminal Justice Lead, College of Policing

Nadine Dinnall – Staff Officer, HM Inspectorate of Constabulary and Fire & Rescue Service

Zoe Gascoyne – Deputy Director, Fraud Investigative Services, HM Revenue and Customs

Rob Jones – Director General (Operations), National Crime Agency

Richard Las CBE – Chief Investigation Officer & Director, HM Revenue and Customs

Nicolle Ndiweni – Police and Crime Commissioner for Derbyshire

Stephen Parkinson – Director of Public Prosecutions, Crown Prosecution Service

Alexandra Robson – Manager, Financial Conduct Authority

Anthony Rogers – Interim Chief Inspector, HM Crown Prosecution Service Inspectorate

Alex Rothwell – Chief Executive Officer, National Health Service Counter Fraud Authority

Kathryn Stone OBE – HM Inspector, HM Inspectorate of Constabulary and Fire & Rescue Services

Matthew Wagstaff – Director of Legal Services, Serious Fraud Office

Legal Expert Panel

Jonathan Ashley Norman KC

Adrian Darbishire KC

Shula De Jersey

Stephen Gentle

Sara George

Sir Max Hill KC

Louise Hodges

Hannah Laming

Jason Lartey (Vice Chair, LCCSA)

Tim Owen KC

Helena Wood – Cifas

Judicial Sub-Group

His Honour Judge Michael Bowes KC

His Honour J Paul Farrer

Her Honour Judge Sally Hales KC

The Honourable Mr Justice Mark Wall

26. Annex D – Glossary

Action Fraud – The UK's former national reporting centre for fraud and cybercrime, now being replaced by the Fraud and Cyber Crime Reporting and Analytics Service (FCCRAS).

Artificial intelligence (AI) – A computer model that can undertake tasks that traditionally required human input, such as evaluating and analysis.

Caveat emptor – A legal principle meaning 'let the buyer beware', historically used to limit liability in fraud cases.

Common law offence – A crime developed through judicial precedent rather than statute, such as conspiracy to defraud.

Computer Misuse Act 1990 (CMA) – Criminalises unauthorised access to computer systems and data.

Confirmation of Payee (CoP) – A banking tool that checks account names to prevent misdirected payments and fraud.

Conspiracy to defraud – A common law offence involving an agreement between two or more people to dishonestly deprive another of property or rights.

Criminal Justice Act 1987 (CJA) – Established the Serious Fraud Office (SFO) and granted powers to compel evidence in serious fraud investigations.

Criminal Procedure and Investigations Act 1996 (CPIA) – Sets out rules for disclosure and investigation duties in criminal cases.

Criminal justice system – The criminal justice system in England and Wales is made up of several separate agencies and departments which are responsible for various aspects of the work of maintaining law and order and the administration of justice. The main agencies of the criminal justice system include:

a. Police Forces.

b. Other law enforcement agencies (i.e. the Serious Fraud Office and National Crime Agency).

c. The Crown Prosecution Service.

d. Magistrates' courts.

e. The Crown Court.

f. The Court of Appeal, Criminal Division.

g. The Prison Service.

h. The National Probation Service.

The Home Office, Attorney General's Office and Lord Chancellor's Department are the three main Government departments with responsibility for the criminal justice system, setting the policy framework, objectives and targets.

Crown Court – The Crown Court has unlimited jurisdiction over all criminal cases tried on indictment and also acts as a court for the hearing of appeals from magistrates' courts.

Data-sharing – The exchange of information between organisations to detect, prevent or investigate fraud.

Deferred Prosecution Agreement (DPA) – A legal tool allowing companies to avoid prosecution by agreeing to pay fines and meet conditions.

Deed poll abuse – Fraudulent use of legal name-change procedures to conceal identity or facilitate crime.

Deepfake – AI-generated media that mimics real people's voices or faces, often used in scams.

Disclosure – The legal duty to share relevant evidence with the defence in criminal proceedings.

Disclosure Management Document (DMD) – A structured plan for managing disclosure in complex criminal cases.

Economic crime – Illegal activities committed for financial gain, including fraud, money laundering, bribery, corruption and other offences that undermine economic integrity and trust.

Economic Crime and Corporate Transparency Act 2023 (ECCTA) – Legislation introducing new corporate liability offences and reforming asset recovery.

Economic Crime Levy – A financial contribution required from regulated firms to fund anti-money laundering enforcement.

Failure-to-prevent fraud offence – A corporate offence under ECCTA holding large organisations liable for fraud committed by employees or agents.

Financial Conduct Authority (FCA) – Regulates financial markets and firms, including fraud prevention and reporting.

Fraud Act 2006 – UK legislation defining fraud as a general offence, committed by false representation, failure to disclose, or abuse of position.

Fraud and Cyber Crime Reporting and Analytics Service (FCCRAS) – The new national system for reporting and analysing fraud.

HM Revenue and Customs (HMRC) – Investigates tax fraud and operates a whistleblower reward scheme.

Identity theft – The unauthorised use of someone's personal information to commit fraud.

Independent Review of Disclosure – A government-commissioned review of the criminal disclosure regime, especially in digital-heavy cases.

Ipsos polling – A method used to gauge public opinion; referenced in the report to assess support for whistleblower rewards.

Law enforcement agency – A government agency responsible for enforcing the law (not including the Crown Prosecution Service).

Money muling – The act of transferring criminal proceeds through one's bank account, often unwittingly.

National Crime Agency (NCA) – UK law enforcement body tackling serious and organised crime, including economic crime.

National Economic Crime Centre (NECC) – A multi-agency unit within the NCA coordinating the UK's response to economic crime.

National Fraud Intelligence Bureau (NFIB) – Analyses fraud reports and disseminates intelligence to police forces.

National Fraud Squad (NFS) – A specialist unit of fraud investigators across UK law enforcement agencies.

Online Safety Act 2023 – Legislation imposing duties on digital platforms to prevent and remove harmful content, including fraudulent advertising.

Police and Criminal Evidence Act 1984 (PACE) – PACE and the Codes of Practice set out police powers and procedures for arrest, detention and interviewing of those suspected of having committed criminal offences and for gathering and handling evidence.

Private prosecution – A criminal case initiated by a private individual or organisation rather than the Crown Prosecution Service.

Proceeds of Crime Act 2002 (POCA) – Legislation allowing recovery of assets gained through criminal conduct.

Public–private partnership (PPP) – A collaborative arrangement between the Government and the private sector to tackle fraud and economic crime.

Regulation of Investigatory Powers Act 2000 (RIPA) – Governs surveillance and access to encrypted data in criminal investigations.

Restorative justice – A process allowing victims and offenders to communicate, aiming to repair harm and reduce reoffending.

Serious crime prevention order (SCPO) – A civil order restricting individuals' activities to prevent serious crime.

Serious Fraud Office (SFO) – A UK agency combining investigation and prosecution of serious or complex fraud and corruption.

Specified Anti-Fraud Organisation (SAFO) – Organisations authorised to receive and share fraud-related data under the Data Protection Act.

Victim – Someone who has had a crime committed against them, or someone who is the complainant in a case.

Whistleblower – A person who reports wrongdoing within an organisation, often protected by law.

E03539408

ISBN - 978-1-5286-6210-9