UK Government

FRAUD STRATEGY 2026-2029

Disrupting crime, supporting economic resilience and delivering justice

March 2026
CP 1523

STOP! THINK FRAUD

Government of the United Kingdom

Home Office

Fraud Strategy 2026-2029:

Disrupting crime, supporting economic resilience and delivering justice

Presented to Parliament
by the Secretary of State for the Home Department
by Command of His Majesty
March 2026

CP 1523

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

Enquiries regarding this publication should be sent to fraud.strategy@homeoffice.gov.uk

ISBN 978-1-5286-6251-2

E03551200 03/26

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

1. Ministerial foreword

Fraud is consistently the largest reported crime type in England and Wales. It affects millions of innocent individuals and businesses each year, undermines public trust, and poses a growing threat to our national security and economic resilience. The scale and sophistication of modern fraud demand a new and accelerated response.

This Government is determined to turn the tide. The threat has continued to grow and evolve. Criminals are exploiting new technologies, deploying increasingly sophisticated attacks and operating across borders with increasing impunity. We must match their innovation with our own, to protect our people and defend our economy.

Strong collaboration between Government, law enforcement, industry and civil society is critical to this Strategy. As a crime that touches every part of our society, it is only right that every part of society joins together to fight fraud.

This is not just about reducing crime; it is about restoring confidence. Every pound stolen through fraud is a pound not reinvested in our economy. Every victim is a reminder of why we must act. By delivering this Strategy, we will make the UK a safer place to live, work, and do business, and send a clear message to criminals: there is nowhere you can hide.

S Mahmood

The Rt Hon Shabana Mahmood MP

Home Secretary

The Rt Hon Lord Hanson of Flint

Minister of State at the Home Office

2. Executive Summary

Fraud against individuals and businesses is evolving rapidly and causing significant harm. It devastates victims, erodes public trust, and poses a serious threat to the United Kingdom's national and economic security.

1. The Government has made crime reduction and economic growth central to its Manifesto. Fraud against individuals and business is the largest crime type in the UK and costs our economy £14.4 billion in 2023–2024.[1,2,3,4] Tackling fraud is essential to cutting crime and strengthening economic resilience.

2. Recognising the increasing number of fraud incidents, high value of fraud losses and harm from fraud, the Government's Manifesto set out a clear commitment to deliver a new Fraud Strategy.

3. **The Government will invest over £250 million between 2026 and 2029 to deliver this Strategy, aimed at combatting fraud against individuals and businesses.** This strategy introduces a new system-wide approach that recognises the agility of criminals and the need for wide-raging intervention. Critical to this approach is close collaboration between Government, regulators, law enforcement, national security agencies, industry and nonprofit organisations. This approach is in three parts:

4. **DISRUPT** (pages 14-31)**:** This Strategy outlines our approach to disrupting the tools, methods, systems and vulnerabilities exploited by criminals, making it harder for them to commit all forms of fraud. By investing in earlier intervention, we increase our chance of stopping the fraud before it happens. Interventions include:

   - Launching the public-private **Online Crime Centre** to share data and collaborate on interventions that eliminate online fraud at scale (from Q2 2026);
   - Sponsoring the **Global Fraud Summit** to raise awareness and lead the international response to fraud (Q1 2026); and
   - Collaborating with the **telecommunications, online and financial services sectors** to deliver interventions that address their vulnerability to criminal exploitation (from Q1 2026).

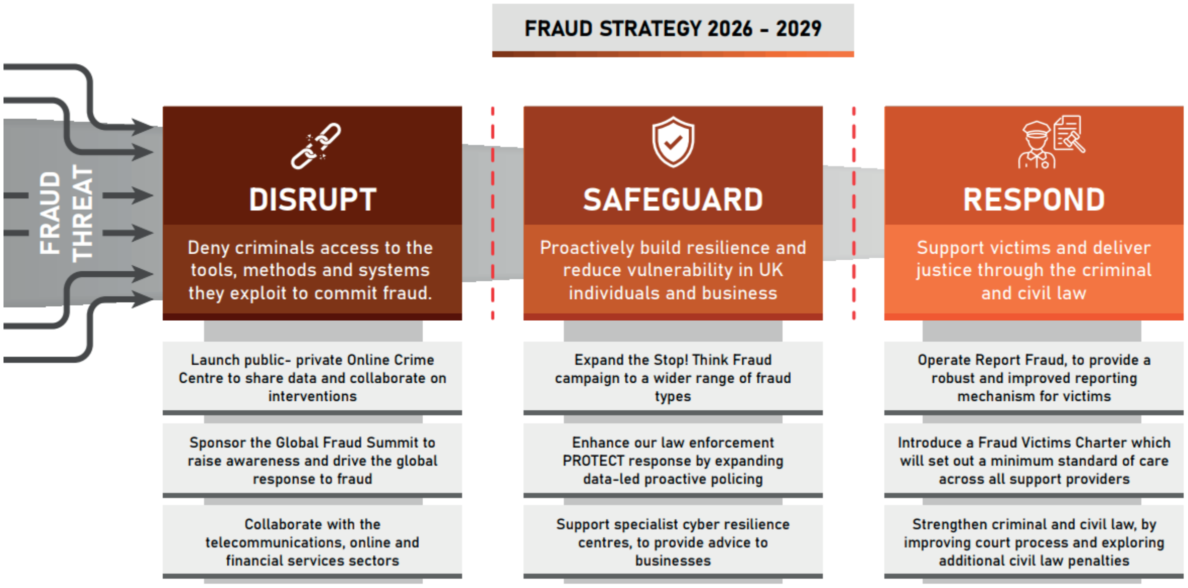
5. **SAFEGUARD** (pages 32-41)**:** Criminals increasingly exploit vulnerabilities in individuals, society, and businesses, many of which shift over time. We will

strengthen resilience so fraud can be detected and repelled before harm occurs. Interventions include:

- Expanding the **Stop! Think Fraud campaign** to a broader range of fraud types, to build individuals' and businesses' resilience to fraud (from Q1 2026);
- Enhancing our **law enforcement PROTECT** response by increasing data-led proactive policing and providing targeted support to at-risk individuals (from Q1 2026); and
- Supporting specialist cyber resilience centres, to provide **advice to businesses** on how to improve their resistance to fraud (from Q1 2026).

6. **RESPOND** (pages 42-53)**:** As fraud grows in scale and complexity, a coordinated, victim-centred response is essential. This pillar brings together reporting, victim support, reimbursement, criminal and civil justice. Interventions include:

- Operating **Report Fraud,** the new, streamlined reporting service, to provide a robust and improved reporting mechanism for victims of fraud (from Q1 2026);
- Introducing a **Fraud Victims Charter** which will set out a minimum standard of care across all support providers, to ensure consistent victim support (Q2 2027); and
- Strengthening **criminal and civil justice**, by improving court process and exploring additional civil law penalties, to ensure criminals face justice (by Q1 2029).



FRAUD STRATEGY 2026 - 2029

DISRUPT

Deny criminals access to the tools, methods and systems they exploit to commit fraud.

Launch public- private Online Crime Centre to share data and collaborate on interventions

Sponsor the Global Fraud Summit to raise awareness and drive the global response to fraud

Collaborate with the telecommunications, online and financial services sectors

SAFEGUARD

Proactively build resilience and reduce vulnerability in UK individuals and business

Expand the Stop! Think Fraud campaign to a wider range of fraud types

Enhance our law enforcement PROTECT response by expanding data-led proactive policing

Support specialist cyber resilience centres, to provide advice to businesses

RESPOND

Support victims and deliver justice through the criminal and civil law

Operate Report Fraud, to provide a robust and improved reporting mechanism for victims

Introduce a Fraud Victims Charter which will set out a minimum standard of care across all support providers

Strengthen criminal and civil law, by improving court process and exploring additional civil law penalties

Figure 1: Fraud Strategy summary diagram

7. This strategy also sets out how the Government will measure and oversee its delivery, supported by a strengthened governance framework based on leadership and accountability across the counter-fraud system. The Fraud Strategy will support the Police Reform White Paper’s commitment on smarter crime prevention and keeping the public safe through its partnership approach to preventing fraud. This includes the Government’s broader plans for Police Reform whereby overall responsibility for Fraud, Economic Crime and Cyber Crime will transfer to the National Police Service (NPS) with the National Crime Agency (NCA).[5] The Strategy also works in parallel with the Public Sector Fraud Authority who lead the Government’s response to fraud against the public sector.

3. The Fraud Threat

The National Security Strategy 2025 identifies fraud as the most common and one of the most corrosive threats facing individuals and businesses in the UK. Fraud, as a technology-enabled hybrid threat, challenges national security, presents an obstacle to growth, and affects society far beyond its immediate victims.[6] Fraud also forms part of a wider network of serious and organised crime, including cyber crime and money laundering.

3.1 The scale of fraud

There are many types of fraud, from those targeting bank accounts, cards, and emerging payment methods, to those operating on online shopping platforms, to others impersonating trusted organisations, brands and individuals, both in person and online.

8. Individuals face a very high risk, with over 4 million offences estimated in the year ending September 2025, representing 45% of all crime in the Crime Survey of England and Wales (CSEW). Around 1 in 14 adults were victims of fraud in this period.[7] The economic and social cost of fraud in England and Wales is significant, reaching at least £14.4 billion in 2023–2024.[8]

9. Scotland shows a similar pattern, with 456,000 offences, or 38% of all offences estimated in the Scottish Crime and Justice Survey 2023/24, making fraud the largest crime sub-type.[9] The equivalent survey in Northern Ireland does not give specific breakdowns for fraud.

10. Businesses and charities also face substantial risk. The Economic Crime Survey 2024 found that 1 in 4 UK businesses with more than one employee experienced fraud in the previous twelve months, amounting to approximately 389,000 businesses and an estimated 6.04 million instances of fraud.[10]

11. Despite a slight drop in fraud between September 2019 and September 2023, fraud is believed to have increased during the COVID-19 pandemic and is growing as a proportion of CSEW crime. In the year ending September 2016, fraud accounted for 31% of CSEW crime and in the most recent data it accounts for 45%. Bank and Credit account fraud rose 36% between years ending September 2023 and 2025.[11]

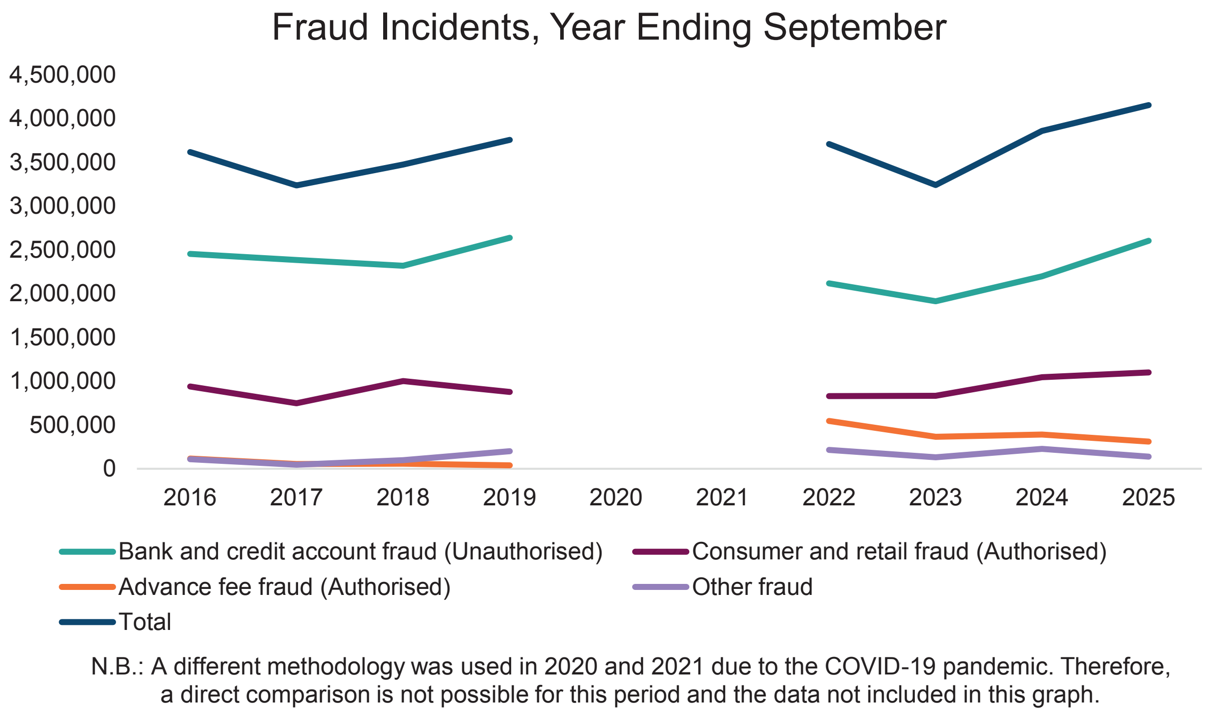


Figure 2: Annual incidents of fraud against individuals from year ending September 2016 to year ending September 2025 Source: CSEW year ending September 2025.[12]

3.2 The impact of fraud

12. Fraud poses significant risks to both individuals and businesses. Victims suffer financial loss and emotional distress, often facing long-term consequences. Businesses experience revenue loss, reputational damage, and increased operational costs. Longer-term, fraud erodes trust, damaging our national financial stability and economic growth.

13. Fraud affects people of all ages and backgrounds. The highest proportion of fraud victims are those aged 45-54 and 55-64 but recent research shows that the risk for young people is growing disproportionately compared to older age brackets.[13,14]

14. Financial losses impact an individual's ability to spend and save, reducing investment and economic productivity. In the year ending March 2024, 74% of frauds involved some financial loss of which 3% lost £10,000 or more.[15] This equates to around 75,000 incidents with losses of £10,000 or more.

15. However, the impact of fraud extends beyond financial loss to include psychological harm which does not always correlate to the amount of money lost.[16] According to a recent survey of fraud victims, 92% experienced emotional or mental health symptoms, 57% experienced a physical health symptom, and 63% experienced behavioural change.[17]

16. Businesses lose money directly, suffer from reduced consumer demand, and face increased defensive costs, limiting their ability to invest and grow. The Economic Crime Survey 2024 found that 10% of businesses, with more than one employee, that had experienced fraud reported a loss of sales or revenue and 2% reported losing a supplier as a result of the fraud.[18] Similarly, charities that have been defrauded can suffer a loss of public trust and a reduction in donations.

17. People and businesses who experience fraud can also become more cautious, reducing their spending and increasing savings or redirecting revenue to protect themselves. Among businesses with more than one employee that had experienced fraud, 8% felt discouraged from carrying out their intended future business activities.[19] Reduced demand and confidence, and significant defensive costs, lead to lost opportunities for revenue and reinvestment.[20,21] Cumulatively, this slows down wider economic growth, especially in sectors reliant on discretionary spending.

18. Whilst criminal methodologies are constantly evolving and adapting, the NCA reported that courier fraud, investment fraud, payment diversion fraud, and romance

fraud remain the fraud types causing the highest harm in the UK in 2025.[22] Although accounting for a comparatively smaller proportion of all fraud targeting UK victims, the financial, emotional, and psychological impacts on victims, and the impacts on the wider economy, are high in these frauds.[23]

3.3 Drivers of the fraud threat

Innovation in technology, the globalisation of organised crime and advances in criminal tactics continue to drive the growth of fraud in the UK. Aided by digitalisation, the abuse of technology has allowed criminals to develop and increase the scale, scope, and speed of their illicit activities.[24] In particular, cyber- and online-enabled fraud is a growing transnational organised crime.

19. Organised Crime Groups (OCGs) and individuals are attracted to fraud, viewing it as a low-risk, high-reward activity. Their intent and capability remain high, and they constantly seek ways to scale up their criminal business models and maximise profits.[25]

20. These groups operate within a broader criminal ecosystem, drawing on organisations offering specialised skills such as illicit marketing and money laundering. They often reinvest the proceeds of fraud to increase the sophistication of their operations and sometimes fund other criminal enterprises, terrorist activity, or hostile state activity.[26]

21. The frauds these criminals commit thrive on connectivity and technology. The UK's reliance on online platforms for banking, shopping and communication has created an environment where criminals can strike without ever meeting their victims. As a result, most frauds now involve transactions carried out by third parties, often without the victim's knowledge.[27]

22. Similarly, fraud and cyber crime are deeply interconnected, amplifying the risks highlighted above for individuals, businesses, and the wider economy. Almost half of all estimated frauds are online-enabled.[28] Criminals exploit data breaches to craft convincing fraudulent emails and text messages, making fraud harder to detect and prevent.[29] The Cyber Security Breaches Survey 2025 estimated 72,000 cyber-facilitated fraud events across UK businesses in the 12 months preceding the survey, with costs ranging from under £100 to over £100,000.[30] These figures show the possibility of catastrophic financial damage. The UK experienced several major data breaches in 2025 which will highly likely create new opportunities for fraud.[31]

23. Phishing sits at the heart of this threat and is likely the most prevalent cyber attack method used by OCGs to target individuals and businesses.[32] Criminals deploy phishing kits and large language models to craft convincing messages and increase

the volume of attacks, embedding fraudulent QR codes in public spaces, and sending phishing emails to harvest personal and financial data.[33]

24. Defensive measures rarely stop criminals for long. Every new control sparks innovation, and OCGs will continue to look for ways to undermine future countermeasures. When two-factor authentication became standard, criminals responded with social engineering techniques to manipulate victims into revealing one-time passcodes and used SIM-swapping to hijack mobile phones. The introduction of spam filters prompted another shift as criminals restructured SMS messages and adopted alternative text formats to bypass firewalls.[34]

25. Technology embedded in daily life offers even more opportunities to target at unprecedented scale. Social media, telecommunications, digital payments and cryptocurrency are now part of routine activity. APP fraud, where victims are deceived into willingly transferring money, illustrates this trend with 53% of reported cases in 2023 involving social media, messaging and call platforms, 13% involving auction/purchase and listing platforms, and 12% involving telecommunications platforms.[35]

26. Criminals are exploiting these platforms and networks to reach their victims easily while concealing their identities. Behind the scenes, the dark web and grey web host marketplaces selling phishing kits and offering fraud-as-a-service subscriptions targeting structural vulnerabilities in these platforms.[36] These services lower barriers to entry, reduce costs, and provide scalable, sophisticated methods to anyone willing to pay.

27. Emerging technologies will continue to shape the fraud threat. Criminals are adopting generative artificial intelligence (GenAI) tools such as deepfakes, large language models, and voice cloning to improve the sophistication, credibility and volume of attacks. They are likely tailoring these tools to specific victims and fraud types, making attacks more effective and harder to detect.[37]

28. Technology is not the only vulnerability. Criminals also exploit historic weaknesses in the UK’s corporate registration system to set up fake companies, lending legitimacy to fraudulent schemes.

29. Similarly, fraud is not confined by borders. Over two-thirds of cases have an international element, making it a global problem with significant cross-border activity.[38,39,40] The UK’s wealth and widespread use of the English language among

criminals make the UK an attractive target. However, international surveys confirm that fraud is rising in many countries.[41]

30. The online nature of many frauds and money laundering methods, including cryptocurrency, often spans multiple jurisdictions, with persistent threats historically from West Africa, Eastern Europe, India, and China. As internet use grows in Western and Central Africa and Southeast Asia, the pool of perpetrators and victims expands.[42] Cyber fraud operations in Southeast Asia are increasingly poly-criminal, intertwined with human trafficking, money laundering, corruption, and organised crime, and remain highly adaptable, relocating compounds or switching jurisdictions to evade crackdowns.[43] This industrialised model of scam compounds is spreading globally, with similar operations emerging in South America and even Europe, with one compound containing dozens of workers recently discovered on the Isle of Man.[44]

31. Overseas fraud networks are highly organised and technologically advanced. Criminals use VPNs and Voice over Internet Protocol (VoIP, where calls are transmitted over the internet instead of phone lines) to mask locations and spoof UK numbers. They deploy artificial intelligence (AI) deepfakes to enhance social engineering, and hack email accounts to divert payments. Many international fraud networks operate from organised call centres or secure scam compounds, demonstrating the industrial scale of modern fraud.

4. Pillar 1: DISRUPT

Effective disruption is essential to tackling fraud. It requires a proactive approach, acting early to deny criminals access to the tools, methods and systems they exploit. This includes maintaining and responding to a detailed understanding of the threat, international collaboration to target criminals wherever they operate, and addressing vulnerabilities in the UK's infrastructure and business practices. This chapter sets out how the Government will strengthen the UK's disruption capability and deny criminals the ability to commit fraud.

4.1 Enhancing the UK's disruption capability

One of the most significant challenges is the perpetual evolution of the fraud landscape. Criminals continue to develop new and increasingly sophisticated fraud types and methodologies. This is compounded by a fragmented data landscape. Partners across the public and private sector have their own unique insights but there is currently no clear, shared, and real-time picture of the fraud threat, meaning collective disruption is delayed or less effective.

32. Therefore, **the Government has committed £31 million to launch the Online Crime Centre (OCC)**, set to begin operations in April 2026. Led by the Home Office and the NCA, and working closely with the City of London Police, the OCC will unite UK policing, the UK Intelligence Community (including GCHQ, the National Cyber Security Centre and the National Cyber Force) alongside private sector partners from the financial, telecommunications, technology, and cyber industries. [45]

33. Bringing together each partner's diverse data, knowledge, and expertise into one place for the first time the OCC is designed to accelerate the UK's response to online crime, initially focussed on fraud and high-volume cyber crime. It will provide the structure and technology to facilitate the sharing of data across different partners, analyse trends and intelligence, and subsequently inform and coordinate high impact law enforcement interventions.

34. The OCC will consist of permanent staff and personnel from across the public and private sectors, conducting its work from fixed locations, and virtually. Where possible the OCC will co-locate with other counter-economic crime teams and industry. It will also benefit from the opportunities presented by the new

Salisbury Square development. Scheduled to open in 2027, Salisbury Square will provide new crime courts to deliver swifter criminal justice outcomes and provide the location of the next City of London Police Headquarters.

35. Enforcement against perpetrators alone will not prevent the widespread harm caused by online fraud and high-volume cyber crime. Through collaboration the OCC will build a comprehensive picture of the tools, methodologies, trends, and perpetrators involved in these crimes. With this understanding, the OCC will share information, identify operational and technical solutions to mitigate harm, and coordinate investigatory and law enforcement actions in the UK and overseas. The OCC will focus on key functions:

36. **Data-Sharing, Analysis and Technology**

- Collecting, combining, and then rapidly analysing large volumes of data across its public and private sector partners. This will inform proactive action to address the online fraud and cyber crime threats, and support private sector partners to improve internal controls and resilience. It will share information relating to criminal abuse of websites, emails, and phone numbers, combined with behavioural data relating to criminals, to identify and disrupt illicit activities by blocking calls, freezing accounts, taking down websites, and restricting social media accounts;
- Sharing information and intelligence with the digital and technology sectors, enabling companies to better protect their customers through their online platforms' trust and safety capabilities; and
- Working closely with the new Report Fraud service and the National Cyber Security Centre's ‘Share and Defend’ capability to deliver a comprehensive system that combines the collection, analysis, and sharing of targeted data for maximum impact.

37. **Reducing Harm**

- Using data to design technical solutions that support industry to put in place controls and processes at the earliest opportunity, reducing vulnerability and denying criminal access to their systems;
- Law enforcement partners, including the City of London Police, NCA, and the UK Intelligence Community, will use the data and information from the OCC to

undermine the enabling technology and services used by persistent offenders of fraud and cyber crime; and

- Working with global partners in the private sector and international policing networks, the OCC will capitalise on these partnerships to share intelligence and collaborate against criminals operating across borders.

38. **Protecting**

- Minimising harm, assist recovery of stolen assets and prevent repeat victimisation. Insights from the OCC will inform industry partners of online fraud trends, guide crime prevention, and provide support on safeguarding customers.

Case Study: Digital Wallets

Tackling online fraud and volume cyber crime is complex. It requires advanced technological capabilities and effective collaboration across government, law enforcement and industry. Despite increasing collaboration in recent years, a lack of central coordination and expertise has often meant criminals have remained ahead of our response.

The OCC will bring together partners to identify threats and provide the data and the environment to collectively develop solutions at pace. For example, digital wallet fraud, where criminals add multiple cards to a device for fraudulent transactions. Here the OCC would act as a data sharing and convening mechanism to identify the vulnerabilities exploited by criminals, and bring partners and data together to develop, test and drive the adoption of solutions. In parallel, where OCC identifies specific criminal operations, targeted interventions such as against fraudulent websites used to advertise stolen card details can be taken to further disrupt criminal groups.

39. Ensuring a strong legal framework for data sharing is critical to the success of the OCC and broader collaboration against fraud. The Data (Use and Access) Act 2025 establishes crime and fraud prevention as a lawful basis for sharing data, supported by forthcoming Information Commissioner's Office (ICO) guidance, but legal uncertainties remain.[46] To address barriers, including cross-border and private sector data sharing challenges, in parallel with the publication of this Strategy **the Home Office is launching a call for evidence on economic crime information sharing.**

Case Study: Takedown of Genesis Market

Genesis was one of the world's largest criminal marketplaces for stolen credentials, hosting over 80 million stolen credentials and digital fingerprints from more than two million victims. Criminals used this data for fraud, including accessing online banking and making unauthorised purchases.

The NCA's National Cyber Crime Unit, working with National Economic Crime Centre and policing partners, shared intelligence nationwide. The operation involved 17 international law enforcement agencies and resulted in 120 global arrests, including 24 in the UK. This takedown removed a major technical infrastructure enabling fraud and significantly disrupted criminal activity.

40. Additionally, to improve wider disruptive efforts, the Home Office will **support law enforcement in leveraging emerging technologies** including trials of AI tools to detect and remove fraudulent websites. For example, the Home Office will work in partnership with the City of London Police and NCA this year to trial the development of an AI tool that supports the investigation and takedown of fraud online.47 This will automate checks of key fraud indicators that help investigators ascertain whether a website is harmful and request its removal. AI is already used by industry to block smishing texts, stop fraudulent transactions, and even deploy scambaiting chatbots. The Home Office will work with industry and regulators to promote safe, responsible use of these technologies to disrupt fraud at scale.

4.2 Tackling fraud at source

The globalisation of the fraud threat presents a major challenge to disruption. Criminal networks and scam centres operate worldwide, often targeting UK individuals and businesses from jurisdictions beyond UK regulation and law enforcement. Stopping these transnational organised criminals from targeting the UK requires international collaboration with countries that experience a high volume of fraud, and those where these gangs operate.

42. A problem this sophisticated and vast requires global leadership, and the UK reaffirms its commitment to providing this leadership. Building on the inaugural Global Fraud Summit in 2024, **the Government will sponsor the next Global Fraud Summit in Vienna in March 2026** with UNODC and INTERPOL. The event will seek commitments from Member States and industry with action to elevate fraud as a political and business priority, strengthen cross-border enforcement, and develop mechanisms for future cooperation.

43. The Global Fraud Summit will also build on the UK's pivotal role in securing the first UN resolution on fraud under the UN Convention against Transnational Organised Crime in October 2024.[48] This resolution established global standards and highlighted the need for strong international action. Beyond convening, the UK is committed to raising global standards and has funded global research and skills development, including INTERPOL's first Global Financial Fraud Threat Assessment and a UN toolkit on fraud.

Case Study: Disruption in Nigeria

In January 2026, the NCA supported the Nigerian Police Force to take down a scam centre. Using intelligence from Meta, an address was identified and, within days, raided resulting in several arrests. Police enquiries found this centre was conducting a range of operations including investment fraud, romance fraud and financially motivated sexual extortion targeting the UK and US.

44. Bilateral partnerships are also central to tackling fraud at source. Through Memorandum of Understanding (MoU) agreements with Nigeria in April 2025 and Vietnam in October 2025, the UK has set out joint action plans for intelligence sharing, capacity building, and disruption of cross-border networks. **The**

Government will pursue further MoUs and bilateral partnerships with governments in high-priority countries, providing technical assistance, training, and support to strengthen local law enforcement and regulatory frameworks.

Case Study: Disruption in India

In July 2025 the India Central Bureau of Investigation (CBI) raided a fraudulent call centre in Uttar Pradesh, resulting in multiple arrests. In July 2025, the India Central Bureau of Investigation (CBI) raided a fraudulent call centre in Uttar Pradesh, resulting in multiple arrests. This followed groundbreaking collaboration and intelligence sharing between the CBI, NCA, FBI and Microsoft, who worked together to identify the organised crime group, build a case and target the complex IT infrastructure used by the criminals. Over 100 UK victims had been contacted, with total losses over £390,000.

45. **The Government will also continue its use of sanctions to disrupt, deter, and hold to account malign actors operating overseas**, including those involved in abusing forced labour to conduct online fraud. These measures will complement global efforts to pursue criminals and prevent them from exploiting UK citizens.

Case Study: Prince Group Sanctions

In October 2025, the UK, in coordination with the United States, imposed sanctions against the Prince Group network for its involvement in scam centres in Cambodia. Across Southeast Asia, these facilities use forced labour, often under threat of torture, to conduct online fraud including against people in the UK. In parallel, the US Department of Justice unsealed a criminal indictment against the head of the Prince Group.

Asset freezes and travel bans, imposed under the UK's Global Human Rights sanctions regime, have locked the network out of the UK's financial system, frozen London properties with a total value of more than £125 million, and helped protect British nationals. In Southeast Asia, UK and US action has triggered a wave of investigations, forcing illicit businesses to close and unmasking those responsible. The Government of Cambodia has subsequently intensified its own campaign; thousands of foreign nationals have been released from scam compounds.

4.3 Preventing the abuse of the UK's telecommunications infrastructure

While telecommunications infrastructure has transformed connectivity and driven growth, gaps and vulnerabilities have enabled criminals to deliver fraudulent texts and calls to victims at scale. These include some of the highest harm types of fraud, generating lucrative opportunities for criminals. To disrupt fraud, criminals must be denied access to the telecommunications network. Achieving this will require close collaboration between Government, regulators, law enforcement, and the telecommunications industry.

46. The Government recognises progress by the telecommunications sector, including commitments under the first Telecommunications Fraud Charter and firewall solutions that have blocked over a billion fraudulent texts since 2022, as well as cooperation with law enforcement in dismantling major fraud operations such as iSpoof.[49,50] In November 2025, leading firms signed the second Telecommunications Fraud Charter, expanding commitments to intelligence sharing, traceback schemes, network upgrades, AI tools, and improved victim support.[51] **The Home Office will monitor delivery and report to Parliament every six months until the end of 2027**, and along with Ofcom will take further action if progress is insufficient.

47. Effective collaboration is supported by robust regulations enforced by Ofcom. Ofcom has powers under the Communications Act 2003 to ensure that telecommunications services such as mobile messaging services are used effectively, efficiently, and are not misused, for example to facilitate fraud. In October 2025, Ofcom further strengthened these efforts by launching a consultation on new rules to help mobile network providers and business messaging aggregators prevent criminals from sending fraudulent mobile messages.

48. Despite these measures, vulnerabilities remain, including relatively easy access to UK phone numbers with minimal identity checks. Weak verification processes and inconsistent compliance standards allow bad actors to present themselves as legitimate while operating anonymously. To address these risks, the Home Office, working with Ofcom, law enforcement, intelligence agencies, and industry will **launch a Call for Evidence in 2026 on proportionate measures to reduce anonymity and strengthen accountability** within the UK communications sector.

49. The aim of the Call for Evidence is to assess the scale of the challenge and gather views on a range of interventions which may include, but are not limited to options such as: registration or licensing regimes for entities providing access to UK networks requiring adherence to Ofcom’s General Conditions and UK incorporation, enhanced Know Your Customer (KYC) requirements, restrictions on anonymous access, and improved law enforcement monitoring. Subject to the evidence presented, the Government and/or Ofcom will undertake a full consultation later in 2026 to build on the existing regulatory approach in a layered and proportionate manner.

50. **The Home Office will also develop options to create a secure digital tool to manage UK telephone numbers** in 2026. The aim is to create, for the first time, a centralised repository that provides real-time information on the status and ownership of numbers. This would give telecommunications companies the power to trace the origin of suspicious activity and more effectively block fraudulent calls before they reach the public.

51. Building on these interventions, transparency of both the prevalence of fraud and the sectors’ response to it is critical to driving accountability. The Government will work with the telecommunications sectors, as well as relevant regulators, to **develop and better utilise data sets and metrics which will track sectors’ performance in tackling fraud**. These data sets and metrics will also inform any required further intervention by Government. A similar approach will be adopted for the technology and financial services sectors.

4.4 Preventing the abuse of the UK’s online infrastructure

While online platforms have driven our digital economy and innovation, vulnerabilities have enabled criminals to target victims at alarming scale. Some of the highest volume and harm frauds occur through fraudulent content, such as marketplace listings, and through fraudulent adverts. To combat fraud effectively, criminals must be denied access to these digital systems. Digital platforms and companies have a responsibility, working closely with Government, law enforcement and regulators, to ensure their platforms cannot be exploited.

52. The Government welcomes progress by the technology sector including through the Online Fraud Charter, signed in 2023, which united major platforms to strengthen processes against fraudulent content and adverts and improve collaboration with law enforcement.[52] Since then, data sharing and collaboration between platforms and other sectors has increased, but broader progress remains uneven and significant weaknesses persist on some services and platforms.

53. Criminal abuse of the online advertising industry presents a major challenge to the UK’s digital economy. A healthy advertising market is a growth engine for the UK, but it is increasingly polluted by fraud and misinformation, undermining trust and harming consumers and legitimate businesses. Criminals are able to hijack the online advertising ecosystem to anonymously promote fraud, distribute malware and launch phishing attacks whilst avoiding detection. This includes the use of sophisticated technologies to bypass existing advertising security measures, such as cloaking, whereby cybercriminals hide the harmful nature or true destination of an advert/web link from scanning environments and security tools. These methods facilitate some of the highest harm types of fraud, including investment frauds, which can cause significant losses to victims and reimbursing institutions.

54. To tackle this, the Online Safety Act introduced fraudulent advertising duties, which make services designated by Ofcom as Category 1 or Category 2A services responsible for using proportionate systems and processes to prevent individuals encountering paid-for fraudulent adverts.[53] **Ofcom aims to consult on the detail of these measures around summer 2026, and we expect the fraudulent advertising duties to come into force in 2027**. Ofcom has the power to impose fines of up to £18m or 10% of qualifying worldwide revenue (whichever is greater) where they find non-compliance with Act duties. In the most serious cases

of non-compliance, Ofcom will be able to seek a court order to impose business disruption measures, which may require third parties (such as providers of payment or advertising services, or Internet Service Providers) to withdraw, or impede access to their services to the non-compliant service.

55. However, vulnerabilities remain in the wider programmatic advertising system, which largely falls outside the current scope of the Online Safety Act. The decentralised nature of the programmatic system, with real time auctions and limited verification checks or transparency measures for online advertisements allows sophisticated criminal actors to insert themselves into legitimate channels. Consequently**, the Home Office and the Department for Culture, Media and Sport (DCMS) have launched a new industry partnership with the Internet Advertising Bureau UK (IAB UK),** under the Online Advertising Taskforce, to improve transparency and tackle malicious advertising, reporting back to ministers in early 2027. However, if industry partnership and market incentives alone remain insufficient to drive improvements, the Government will take legislative action within this Parliament.

56. Beyond advertising, online communications, including on social media, present opportunities for criminals to target the public at scale. Since March 2025, the Online Safety Act has placed duties on in-scope platforms to prevent, minimise and remove illegal and fraudulent user-generated content, while also mandating routes for trusted flaggers to report illegal content directly.[54] Ofcom has committed to robust monitoring and evaluation of the impact of the Act, focused on two core questions: first, what changes are services making to comply with their duties under the Act; second, are these changes translating into a safer life online for UK users. This will allow Ofcom to adapt their strategic priorities and Codes of Practice based on what works well and where further action is needed. Ofcom's findings will be shared via their annual reports, transparency reports, statutory reports and research papers.

57. Whilst under the scope of the Online Safety Act's content duties as detailed above, the Government recognises that criminals specifically continue to exploit online marketplaces, particularly those that facilitate peer-to-peer transactions. APP frauds on auction and purchase listing platforms cost the UK public £21.3m in 2023, whilst the Payment Systems Regulator estimated that almost 1 in 10 of all UK adults have fallen victim to a purchase fraud.[55,56]

58. As well as the Online Safety Act, the Digital Markets, Competition and Consumers Act 2024 strengthens protections by banning fake reviews and enhancing

enforcement powers for the Competition and Markets Authority.[57] Together, these measures aim to address fraud in digital markets. Through ministerial oversight, **the Government will continue to monitor and evaluate the effectiveness of existing regulations and enforcement powers** in addressing harms in digital marketplaces, including fraud. If further measures are judged to be needed to protect consumers, the Government will act.

59. As set out above, **as with the telecommunications sector, the Government will develop and better use metrics and data sets to drive accountability in the online industry**. For the online industry this includes, but is not limited to, the duty to publish transparency reports under the Online Safety Act.

60. As is the case with online platforms and services, the rapid development of artificial intelligence brings both opportunities and risks. To address these, **the Government is working to improve the security of AI models** and ensure their safe adoption to drive growth. A key threat is generative AI's ability to create deepfakes that impersonate trusted individuals and organisations. To counter this, the Home Office is leading work with the Department for Science, Innovation and Technology (DSIT), the Alan Turing Institute and other Government departments to design and implement a robust framework for detecting deepfake media, including fraudulent documents and synthetic audio. As part of that work, in January 2026 the Government hosted the Deepfake Detection Challenge 2026, with support from Microsoft, bringing together technical experts to better understand current and emerging threats. The Home Office will continue to help protect the public from harmful and deceptive content by evaluating detection capabilities to ensure that they remain effective against emerging techniques.

4.5 Preventing the abuse of the UK's financial flows

The UK's financial services sectors and emerging payment and cryptoasset technologies have driven growth and created business opportunities. They are also often the last line of defence in disrupting criminals' attempts to commit both unauthorised and authorised frauds. While the sector has invested heavily in fraud prevention, vulnerabilities remain. To drive down and disrupt fraud, we must address the persistent threat of unauthorised fraud, raise best practice, strengthen customer protections, and cut off the criminal opportunities presented by cryptoassets.

61. The financial services sector has taken significant steps to combat fraud, including but not limited to the Retail Banking Fraud Charter of 2021, the introduction of Confirmation of Payee and the Banking Protocol.[58] Since October 2024, banks have been mandatorily reimbursing losses where victims are deceived into willingly transferring money (APP fraud). In the first year of the scheme, 88% (£173m) of money lost to in-scope APP fraud was reimbursed to victims. [59]

62. Despite these strong defences, at least £629.3 million was stolen in the first half of 2025 alone.[60] Of this total, the majority consisted of unauthorised fraud types accounting for £371.8 million. [61] Bank and credit account fraud rose 19% to 2.6 million cases in the year ending September 2025. [62]

Case study: Reimbursement

Yara was defrauded while trying to rent a property advertised on social media. Believing the person posing as the landlord was legitimate, she signed a subletting agreement drafted by a real law firm and paid £10,000 in deposits and rent. The criminal had previously stayed in the property, stolen the landlord's documents, and used them to deceive the law firm. After discovering this, Yara reported the situation to her bank, which confirmed the fraud and reimbursed her losses, minus a £100 claims excess.

63. Unauthorised fraud levels have remained consistently high and continue to pose a persistent challenge for counter-fraud efforts, but the underlying drivers are still unclear. To address this, **the Home Office will launch a Call for Evidence focused on unauthorised fraud** in 2026. Assessing the scale, drivers and enablers of

unauthorised fraud, it will generate an improved evidence base and potential next steps by the end of 2026.

64. Greater focus will also be placed on setting clear examples of good and poor practice in tackling authorised fraud. Building on existing work, **the Financial Conduct Authority (FCA) will consider examples of practices for preventing APP fraud and money mule activity and will share its recommendations** with the financial services sector.

65. The Government is aware of the emerging and concerning vulnerability presented by the criminal use of technologies and social engineering tactics to gain access to consumer and business accounts, including the use of deepfakes. Customer authentication and account security is a vital step in cutting off these avenues for criminals, including the use of effective Know Your Customer (KYC) and Customer Due Diligence (CDD) processes.

66. However, as criminals adapt, it is vital to continuously improve security protocols. To enable this, HM Treasury will repeal the existing Strong Customer Authentication technical standards, **allowing the FCA to incorporate key standards into its rules and adopt a more agile, outcomes-focused approach**, as soon as Parliamentary time allows. This will support the adoption of new technologies, enabling firms to implement innovative, continuously improvable authentication methods that better protect payments and accounts, while applying proportionate, risk-based measures for low-risk transactions.

67. To further improve the security of consumer accounts, **the National Cyber Security Centre (NCSC) will continue to work with standards bodies, technology providers, and industry partners to accelerate the adoption of passkeys.** Passkeys offer a more secure and user-friendly alternative to traditional passwords and multi-factor authentication.[63] They are unique to each account, cannot be guessed, are phishing resistant, and are easier and faster to use. The Government will also promote best practice using NCSC guidance on strong authentication, including passkeys, and certified Digital Verification Services under the UK Digital Identity and Attributes Trust Framework. Regulators and financial institutions are encouraged to adopt this guidance to strengthen anti-money laundering controls. Aligning secure technology, clear standards, and public awareness will create a safer digital financial environment.

68. Cryptoassets pose growing risks, with investment fraud among the fastest-rising threats.[64] The NCA launched a nationwide campaign in 2025 to help consumers spot fraud, and the Government is also supporting law enforcement, including the Serious Fraud Office (SFO), to enhance cryptoasset investigation capabilities.

69. The Government is further intervening by adapting regulation to keep pace with these emerging technologies. Since 2023, firms marketing cryptoassets to UK consumers have been required to comply with the FCA's Financial Promotions Regime, ensuring that all promotions are fair, clear, and not misleading. In December 2025, HM Treasury introduced legislation bringing cryptoasset firms under a full financial services regulatory framework, similar to traditional financial firms.[65] Once the regime comes into force in October 2027, **cryptoasset firms will need to be authorised by the FCA and to comply with its rules**. The new regime covers 'fungible and transferable' cryptoassets and creates new regulated activities such as operating a qualifying cryptoasset trading platform and issuing a qualifying stablecoin in the UK.

70. As set out for the telecommunications and online industry above, **the Government will use data and metrics to track performance** to drive accountability in the financial services industry, building on the existing rich data picture.

4.6 Combatting fraudulent businesses and practices

Fraudulent business practices are an insidious driver of fraud in the UK, with criminals exploiting loopholes, creating fake companies and impersonating legitimate organisations to deceive and exploit. These actions inflict direct losses on businesses and consumers, while also eroding trust and stability across the wider economy. The Government is determined to disrupt those who abuse corporate structures for criminal gain and shield legitimate businesses from such exploitation.

71. Verifying the legitimacy of partners, suppliers and customers is a core challenge for businesses and charities, with many relying on Companies House data. Historically, the register has operated largely on trust, creating opportunities for criminals to register fake companies or manipulate records. The Economic Crime and Corporate Transparency Act 2023 introduced reforms including mandatory identity verification for directors, persons with significant control, and those filing information with Companies House.[66, 67] It also introduced enhanced powers for the Registrar to check, remove and decline information, share data and take enforcement actions, and the authority for the Registrar to strike off companies set up for unlawful purposes.[68] These have the aim of improving reliability of the companies register and reducing abuse of UK corporate structures.

72. Enforcement is also being strengthened alongside these reforms. The Insolvency Service's new Investigation and Enforcement Strategy expands its focus to fraud and money laundering facilitated through companies, using civil and criminal powers to investigate, wind up companies, disqualify directors, and pursue offences under relevant legislation. HMRC, Companies House, and the Insolvency Service have also agreed a joint implementation plan to close vulnerabilities in company registrations and dissolutions, increase the compliance impact achieved by HMRC, and refer more cases of unfit directors for investigation. Progress on this plan will be reported to the National Audit Office in 2026. In addition, the 2025 Budget also provided funding for **a new Abusive Phoenixism Taskforce** from 2026 within the Insolvency Service to investigate phoenixism, where individuals use companies repeatedly to evade debts or for fraudulent purposes.[69]

73. The impersonation of legitimate organisations within a business's supply chain is a threat to companies. Criminals intercept legitimate emails and send fake invoices

with losses ranging from hundreds to millions of pounds.[70] To address this, **the Government will mandate electronic invoicing for all VAT invoices** from April 2029, publishing a roadmap at Budget 2026. Electronic invoicing will allow suppliers to generate and send invoices through secure digital systems, reducing interception risks. **The Government will also consider digital company identities** as a way to secure electronic identities and streamline verification of onboarding, transactions, and compliance, building on the blueprint produced by the Centre for Finance, Innovation and Technology (CFIT) and backed by HM Treasury and leading industry figures.[71]

74. The Government also recognises fraud can be committed by corporates. The Economic Crime and Corporate Transparency Act 2023 introduced a new corporate offence of 'failure to prevent fraud', effective from September 2025.[72] Large organisations must now implement procedures to prevent fraud by associated persons. Guidance has been issued by the Crown Prosecution Service (CPS), SFO, Home Office and Scottish authorities to support enforcement and self-reporting.[73,74,75]

4.7 Summary of Disrupt actions

75. **Enhancing the UK's disruption capability:**

- The Home Office will launch the new Online Crime Centre (in 2026);
- The Home Office will launch and publish a response to a Call for Evidence to identify barriers to effective data sharing (in 2026); and
- The Home Office will continually support law enforcement to leverage emerging technologies to combat fraud.

76. **Tackling fraud at source:**

- The Home Office will sponsor the next Global Fraud Summit in Vienna in March (in 2026);
- Government will continually pursue memoranda of understanding (MoUs) with high-priority countries; and
- Government will increase its use of sanctions to hold to account malign actors operating overseas.

77. **Preventing the abuse of the UK's telecommunications infrastructure:**

- Government will oversee and closely scrutinise signatories' performance against the telecommunications charter (by 2028);
- Home Office will launch a Call for Evidence on proportionate measures to reduce anonymity and strengthen accountability (in 2026);
- The Home Office will begin developing options to create a secure digital tool to manage UK telephone numbers (in 2026); and
- Government will develop metrics for measuring prevalence of fraudulent activity across telecommunications networks, and their performance in removing and/or blocking such activity.

78. **Preventing the abuse of the UK's online infrastructure:**

- Ofcom will introduce the Fraudulent Advertising Duty into force (in 2027);
- The Home Office and the Department for Culture, Media and Sport (DCMS) have launched a new industry partnership to address fraudulent advertising, reporting back and, if required, prepare legislation within this parliament (in 2027);

- Government will continually monitor effectiveness of regulation and enforcement powers on online marketplaces;
- Government will develop metrics for measuring prevalence of fraudulent activity on online platforms, and their performance in removing and/or blocking such activity; and
- Government will continue to work with the tech sector to take action to improve the security of AI models.

79. **Preventing the abuse of the UK's financial flows:**

- The Home Office will launch a Call for Evidence focused on the causes of unauthorised fraud (in 2026);
- The FCA will share best practice recommendations in relation to APP fraud and exploitative money laundering;
- HM Treasury will repeal the existing Strong Customer Authentication technical standards, allowing the FCA to incorporate key standards into its rules and adopt a more agile, outcomes-focused approach (as soon as Parliamentary time allows);
- The National Cyber Security Centre will continue to work with standard bodies and technology providers to accelerate the adoption of passkeys;
- Regulate cryptoasset financial activities by requiring cryptoasset firms to obtain FCA authorisation and comply with its rules (in 2027); and
- Government will develop metrics for measuring the prevalence of fraudulent activity in financial services, and their performance in removing and/or blocking such activity.

80. **Combatting fraudulent business practices:**

- Government will set up a new taskforce within the Insolvency Service to tackle abusive company phoenixism, as announced in the 2025 Budget (from 2026);
- Government will mandate electronic invoicing for all VAT invoices (from 2029); and
- The Government will consider digital company identities as a way to secure electronic identities and streamline verification of transactions.

5. Pillar 2: SAFEGUARD

The pervasive nature of fraud means that a level of crime will likely evade our disruptive efforts, necessitating a second line of defence that safeguards individuals and businesses. Safeguarding involves proactive action to reduce vulnerability and build resilience, by ensuring criminals are unable to find potential victims, and that individuals and businesses have the knowledge and tools to recognise and avoid fraud. This pillar sets out how Government will safeguard individuals and business by building an informed society, providing targeted support to those most vulnerable, and addressing the risk of financial exploitation.

5.1 Building resilience

Effective communication and public education are critical to building a society resilient to fraud. Given the growing and evolving nature of the fraud threat, this cannot be stagnant or focus on a single demographic. Rather, it must pre-empt and respond to the threat.

81. The Stop! Think Fraud campaign is a national behaviour-change initiative helping individuals and small businesses identify and prevent fraud.[76] From April 2026, the campaign will **expand to cover a broader range of fraud types including high-harm frauds**, strengthen its advice for small businesses by working with trusted partners such as the Federation of Small Businesses, and explore technology to improve guidance accessibility. The broader ambition for Stop! Think Fraud is to continue to work with industry, including financial services, technology and telecommunications companies, to encourage the uptake of protective behaviours by integrating messaging into their customer communications and delivering joint activity.

82. Tools that help to identify whether emails, texts, websites or QR codes are genuine can also help to build widespread resilience. From 2026, **the Home Office will also work with a range of partners to raise awareness of existing tools that the public can use to help detect and protect against fraud**. This will help individuals to identify and make use of the range of services that are available, some of which are embedded within tech, telecommunications, and banking platforms, to help protect themselves more effectively.

Case Study: Stop! Think Fraud Industry Collaboration

Ticket fraud occurs year-round, but criminals exploit major events. This includes the Premier League kick-off in August. Over the past two seasons, more than 2,400 cases of football ticket fraud were reported to Lloyds, with losses exceeding £500,000. Recognising the value of working together to jointly warn football fans, Lloyds and the Government's Stop! Think Fraud campaign collaborated ahead of the 2025 Premier League season to equip fans with the knowledge and tools to stay protected from fraud when buying tickets. The activity reached people through national, regional and online news channels, alongside social media influencers.

83. Effective resilience must start at a young age. Young people are increasingly targeted through social media and online gaming. A recent study found that 96% of 13–18-year-olds transact online, with 68% making purchases independently. Of those spending money on online purchases, 14% believe they have been defrauded in some way.[77] To address this, the Department for Education will embed financial, media and digital literacy in the revised curriculum and the Home Office will work with the South West Regional Organised Crime Unit (SWROCU) and the Personal, Social, Health and Economic Association (PSHE) to **embed free educational resources about fraud and exploitative money laundering for school-aged children** in England from the 2026/27 academic year. The Government will also use the Fraud PROTECT Network (see paragraph 89) to **support university students' resilience to fraud and exploitative money laundering** from 2026 by providing fraud education on campus and through student communities.

84. Whilst preventing fraud committed by external actors requires education, preventing fraud committed by someone known to the victim requires deeper, targeted safeguards, especially given the overlaps with economic abuse. In 2026, the Home Office will lead a dedicated working group with representation across government departments, law enforcement, industry, legal experts and the third sector to **develop a system-wide response to protect individuals at risk of abuse of position**, building the resilience of vulnerable and elderly people who depend on legal protections such as power of attorney.

85. Businesses experience specific fraud and cyber risks which require targeted intervention and resilience building. The National Cyber Security Centre (NCSC) provides comprehensive support, including the Cyber Action Toolkit, a starting point for small organisations and a step towards Cyber Essentials certification, the recommended minimum standard. [78,79] Additional NCSC schemes, including Cyber Incident Exercising and Cyber Incident Response, help organisations defend, respond to, and recover from attacks. The Charity Commission has worked with the NCSC to develop cyber and fraud guidance specifically for charities.[80]

86. The Home Office will also **continue to support regional Cyber Resilience Centres across England and Wales**, led by the City of London Police, providing tailored support to small businesses and promoting secure supply chains through the Cyber Essentials Scheme and Ambassador Programme.[81] Similar initiatives operate in Scotland and Northern Ireland through the CyberScotland Partnership and the Northern Ireland Cyber Security Centre.

87. Organised crime gangs also infiltrate businesses to commit large-scale financial fraud. To counter this, the Better Hiring Institute, CIFAS and Higher Education Degree Datacheck have produced guidance to help businesses strengthen recruitment processes.[82]

5.2 Reducing vulnerability

Criminals excel at identifying circumstances that increase vulnerability to fraud and a change in circumstance can increase an individual or business' likelihood of becoming a victim. Therefore, in addition to building resilience, proactive steps must also be taken to identify those who may have heightened vulnerability and provide support before they are targeted.

88. The PROTECT Network, made up of local, regional, and national law enforcement officers, is critical to safeguarding individuals against fraud and cyber crime. The network works across England and Wales to deliver consistent and targeted fraud messaging into communities to mitigate the threat of fraud and revictimisation.

89. Better data allows for more informed and targeted intervention to protect those most vulnerable. The Home Office and law enforcement are developing data-driven methods to identify fraud hotspots and deliver targeted prevention advice. Building on the Project Aegis pilot and Operation Callback (see case study below) and using richer data from the City of London Police's new Report Fraud service, the **Government and law enforcement will deliver proactive, intelligence led PROTECT activities in local areas** from 2026. This will deliver targeted, practical advice to prevent victimisation.[83]

Case Study: Project Aegis

Between February and September 2025, Project Aegis, a Home Office pilot led jointly with City of London Police, was undertaken across Thames Valley, Greater Manchester and Southern Wales supported by local and regional police. The pilot tested a proactive, intelligence-led approach for preventing fraud victimisation. Using a 'hot spotting' model, officers and volunteers visited high risk neighbourhoods identified through a London School of Economics data model based on Action Fraud reports. Interventions focused on online shopping and investment fraud.

The pilot involved two phases, with approximately 5,600 properties visited. Officers engaged residents through door-to-door conversations and distributed materials to raise awareness and build confidence in spotting fraud.

Case Study: Operation Callback

From February to April 2025, the Metropolitan Police Service ran Operation Callback across London, with a victim-based focus in Bromley, Croydon, and Sutton. Using a hotspot approach, the campaign combined multi-agency collaboration and targeted communications to prevent courier fraud.

Key actions included distributing 115,000 prevention leaflets, 94 awareness visits, 40 presentations to nearly 2,000 people, and installing 50 call blocking devices. Outreach extended to banks, jewellers, post offices, and community groups. Public engagement was strong, with social media reaching 31,000 views and 100% of surveyed attendees pledging behaviour change. Within the focus area, offences resulting in financial loss were reduced by 50%, and associated losses decreased by 67%. Callback 2 has since been launched to sustain and further strengthen prevention and disruption efforts.

90. To deliver a consistent and effective service for vulnerable individuals, from 2026 **the Home Office will work with City of London Police to align the Fraud and Cyber PROTECT networks** improving efficiency by reducing the current levels of duplication and overlap, whilst preserving specialist skills. From 2026, **Police Support Volunteers will also play a greater role as Fraud and Cyber Volunteers**, building on the current 146 volunteers in post to reach lesser-served communities. These volunteers will bring valuable expertise to support law enforcement and deliver consistent, nationally aligned advice, boosting capacity across the PROTECT network.

91. Data held by industry about their customers and users can also help identify when someone may be at risk. Therefore, **the Home Office will improve how the PROTECT Network receives and responds to notifications from industry** from 2026. For example, tech platforms will be encouraged to proactively alert the PROTECT Network when they identify suspected fraud victims, enabling officers to contact those individuals with tailored advice or share intelligence with their banks to put safeguards in place.

92. The current financial safeguarding response is often inconsistent. We will therefore continue to support UK Finance to expand their Vulnerable Victim Notification Scheme to all police forces.[84] This will allow law enforcement to flag concerns about an individual's financial vulnerability directly to the financial services sector, enabling

tailored safeguards to be applied before fraud or revictimisation occurs. **The Home Office will then launch this as a Financial Safeguarding Scheme** by identifying opportunities to expand the initiative to frontline professionals, including victim care services, and establish clear referral pathways for those at risk. This will help deliver a more consistent, coordinated approach to safeguarding vulnerable people across the entire system.

93. To support rollout, **the Government will provide additional funding to the National Trading Standards for new posts in their Scams Team**. These roles will coordinate the multi-agency approach to fraud implementation across all police force areas, pooling data and resources to ensure consistency and deliver better outcomes for victim support, awareness and communications.

5.3 Combatting financial exploitation

Financial exploitation remains a major factor in many fraud cases and therefore warrants a unique safeguarding approach. Criminals often target individuals who are emotionally or financially dependent, using established trust to manipulate victims to access money or assets. A bespoke approach to combatting financial exploitation will add an additional layer to the safeguarding response.

94. Criminals frequently coerce victims into laundering proceeds of crime or committing fraud-related offences. 'Exploitative money laundering' has serious consequences for vulnerable individuals, especially children and young people. It also forms a vital part of criminal business models and their ability to withdraw or release stolen funds ('cash-out') so it can be used without detection.[85]

95. To address this, the Home Office, the NCA and FCA have published nine economic crime priorities for the UK, including tackling exploitative money laundering.[86] To aid the public and private sectors, the **FCA will analyse 'cashing-out' methods and share their findings with industry, while also identifying barriers to tackling exploitative money laundering and developing targeted solutions.** In parallel, Ipsos research commissioned by the Home Office has examined individuals understanding of money muling, how individuals become involved and exit pathways. This is due to be published in 2026.

96. Recognising the significant harm that financial exploitation can cause, **the Home Office will work with The Children's Society to identify and establish a clear referral pathway for victims of financial exploitation related to exploitive money laundering.** This pathway will help frontline professionals identify children and young people who require support, and route them to the appropriate safeguarding response. By doing so, we will ensure vulnerable individuals receive the protection and assistance they need.

97. To reinforce these measures, national coordination of fraud prevention activity will also be strengthened from 2026 to align more closely with the cyber crime response, strengthening efforts to disrupt exploitative money laundering and embed best practice. **A dedicated Fraud PREVENT lead within City of London Police will drive strategic coordination across law enforcement, Government, and partners**. The role will also coordinate targeted education and interventions for individuals at risk, including those using online platforms for offences such as

carding, whereby credit card information is illegally obtained, trafficked or used without authorisation.

Case Study: Financial exploitation

At 15, Ace was placed in care after experiencing neglect and trauma. Whilst living in a children’s home, he was groomed online and coerced into financial fraud, including money laundering and using stolen credit cards. His carers raised concerns with police, children’s social services and made a referral to The Children's Society.

The Children’s Society built trust with Ace and identified him as a victim of financial exploitation. He shared his shame about being manipulated and threatened by criminals. The Children’s Society provided emotional support, safety advice, and disruption strategies, while advocating for safeguarding action and helping professionals understand the abuse Ace experienced. A multi-agency safety plan was created to safeguard Ace, and after a year he felt safer, more confident, and better able to recognise exploitation and seek help.

5.4 Summary of Safeguard actions

98. **Building resilience:**

- The Home Office will strengthen the Stop! Think Fraud campaign to a broader range of fraud types (from 2026);
- The Home Office will work with the private sector to develop impartial and comprehensive consumer advice from (2026);
- The Home Office will embed educational resources for school-aged children in England (from 2026);
- The PROTECT network will support university students' resilience to fraud and exploitative money laundering (from 2026);
- The Home Office will work with key stakeholders to develop a system-wide response to protect individuals at risk of abuse of position (from 2026); and
- The Home Office will continue to support the regional Cyber Resilience Centres.

99. **Reducing vulnerability:**

- Law enforcement will deliver proactive, intelligence led PROTECT activities in local areas (from 2026);
- The Home Office will support the alignment of the Fraud and Cyber PROTECT network (from 2026);
- The Home Office will support law enforcement to leverage police support volunteers (from 2026);
- The Home Office and law enforcement will work together to improve how the PROTECT Network receives and responds to notifications from industry (from 2026);
- The Home Office will launch a Financial Safeguarding Scheme (from 2026); and
- The Home Office will fund the National Trading Standards scams team to support the multi-agency approach to fraud (from 2026).

100. **Combatting financial exploitation:**

- The FCA will conduct analysis of 'cashing-out' and work with industry to tackle money laundering;

- The Home Office will work with The Children’s Society to identify and establish a clear referral pathway for victims of financial exploitation related to exploitive money laundering (from 2026); and
- The Home Office will work alongside the City of London Police to strengthen national coordination of fraud prevention activity (from 2026).

6. Pillar 3: RESPOND

Our approach to fraud cannot only be about prevention, it must also include a strong response when fraud does occur. Fraud leaves victims facing financial loss and emotional distress, as well as damaging business and consumer confidence. This is compounded by low investigation and conviction rates which further undermines trust and risks repeat offending. A robust response includes ensuring victims are recognised and supported, law enforcement is empowered, and criminal and civil justice mechanisms are in place. This pillar sets out how we will improve victims' experience, enhance investigative capabilities, improve international law enforcement collaboration and deliver civil and criminal justice outcomes.

6.1 Improving victims' experience

The primary focus of the Government's response to fraud is ensuring all victims are heard and supported. This means there must be a consistent and accessible reporting mechanism, as well as robust and effective victim care.

101. A victim-centred approach starts with a single, accessible reporting route. The previous national reporting service for fraud (Action Fraud), introduced in 2013, could not manage the levels of fraud that are seen and reported today**.** The **new service Report Fraud, operational from 2026,** ensures an efficient reporting mechanism that enables swifter police intervention and provides better support to victims.

102. Report Fraud uses state of the art technology to provide a more efficient service and will improve victims' experience. With an upgraded call centre and user-friendly website, the new service will simplify reporting, provide clearer updates, and prioritise vulnerable cases for immediate support through Report Fraud Victim Services (formerly the National Economic Crime Victim Care Unit). Report Fraud's new data platform improves the analysis of reports and speeds up referrals to police and other partners to investigate and disrupt criminals, while enhanced performance tracking will ensure continuous improvement.

Case Study: Report Fraud

Victims will be able to seek advice via webchat or chatbot before reporting fraud through a call centre or online channel. An Interactive Voice Response System will prioritise victims into appropriate queues, followed by a logic-based triage to ensure accurate crime coding.

Once a report is submitted, victims receive bespoke protection advice to help prevent re-victimisation and build resilience. Reports will comply with National Crime Recording Standards and Home Office Counting Rules, enabling identification of vulnerabilities, technical enablers for stop/block actions, and opportunities to alert financial institutions for near real-time intervention.

All reports will feed into strategic intelligence assessments under the National Intelligence Model, highlighting threats, targeting methods, and emerging fraud trends. Data will also be uploaded to the Police National Database to ensure compliance and visibility across law enforcement.

103. Once a victim reports fraud, care and advice must be consistent, however, support currently varies by location and service. To address this, **the Home Office will introduce a Fraud Victims** Charter **in 2027**. Developed with victims, law enforcement, support organisations, and industry, the Charter will set national standards for the level of service every victim should receive, including response times, minimum standards of care, and clear communication pathways. It will ensure consistent advice on reimbursement, prevention, and recovery, alongside access to emotional and practical support, all underpinned by accountability measures to ensure compliance. By establishing national standards, disparities in victim care will be tackled and support will no longer depend on geography or organisation.

104. Alongside improving reporting and care standards, Government must address the wider impact of fraud on victims. Financial consequences can be severe, so under the Financial Services and Markets Act 2023, the Payment Systems Regulator introduced mandatory reimbursement for APP fraud within the Faster Payment System from October 2024.[87] The Government remains committed to maintaining mandatory reimbursement. The regulator will keep the scheme under review to ensure it mitigates harm and incentivises firms to prevent fraud.

Case Study: Romance Fraud Victim Support

Jake was twice identified by Essex Police as a potential romance fraud victim. Initially flagged after attempting to buy £400 in gift cards, officers discovered he had already sent £3,500 abroad. Police adjusted his social media settings, provided prevention advice, and referred him to support services, which he declined.

Months later, Jake tried to open a bank account for the person he believed he was in a relationship with and revealed he had sent a further £20,000 in gift cards. A Victim Support case worker helped him recognise that this was fraud using a questionnaire, phone verification, and video call confirmation. Jake acknowledged the fraud, reconnected with family, and received ongoing support from Victim Support and a Fraud PROTECT officer to improve his wellbeing and prevent further harm.

105. Beyond financial loss and emotional distress, many victims also suffer identity theft, which can have lasting psychological and financial effects and create further burdens to resolve issues beyond their control. To address this, **City of London Police will establish referral routes to identity repair services, and the Home Office will explore opportunities to further support fraud victims with an identity repair solution**, working closely with industry, charities and law enforcement. Identity repair solutions assist individuals who have had their identities stolen by helping restore them and preventing further misuse. This work will include working with partners to develop additional guidance, tools and partnerships that can strengthen victims' ability to recover quickly and reduce the risk of repeat harm.

6.2 Enhancing law enforcement investigation capabilities

Fraud as a complex, technology-driven, and often international crime presents a unique challenge for law enforcement. To respond, a bespoke approach is required, one that ensures law enforcement have the tools, training and experience to fully investigate each crime.

106. National coordination is essential to tackle fraud, a complex and widespread crime. The Government recognises the national leadership provided to date by the City of London Police with specialist expertise in tackling fraud and the National Economic Crime Centre within the NCA as the operational system lead. As set out in the Police Reform White Paper, overall responsibility for Fraud, Economic Crime and Cyber Crime will transfer to the new National Police Service with the NCA, and will be the lead agency for these crimes. This will ensure a more streamlined approach with clearer roles and more effective tasking responsibilities.

107. We recognise the specialist expertise of City of London Police in tackling these crimes, including currently hosting Report Fraud and other specialist units and capabilities. Subject to the findings of the Independent Review of Police Force Structures (outlined in Chapter Three of the Police Reform White Paper), the Government will assess whether these specialist services should transfer to the NPS or could be delegated and continue to be delivered by the City of London Police under NPS direction. Whilst these changes are underway, the Government will continue to work with all law enforcement partners to make continuous improvements to the fraud law enforcement response at a local, regional and national level.

108. The National Fraud Squad (NFS) brings together officers from the NCA, City of London Police and Regional Organised Crime Units to deliver intelligence-led investigations targeting the most serious offenders. Leveraging the Online Crime Centre, the NFS will receive higher-quality intelligence packages to proactively disrupt organised criminals before they reach victims, reducing the burden on local forces. To strengthen its impact, the **Home Office will conduct an impact evaluation of the NFS in 2027** and implement improvements across regional and national responses.

109. Better intelligence and tools for law enforcement will accelerate investigations and lead to greater and swifter outcomes for victims. The new Report Fraud service

provides far richer, faster intelligence to local police via the National Crime Analysis System, improving case triage, handling and timely dissemination to forces. Similarly, industry collaboration is also vital for better law enforcement intelligence. By early 2028, **the Home Office will work with Ofcom and industry to develop and implement a National Telecommunications Traceback Scheme**, a process to identify the origin of a suspicious or fraudulent communication across interconnected networks. This will enable investigators to trace fraudulent calls and texts, identify repeat offenders, and present robust evidence for prosecutions and civil action.

110. **The Home Office is also supporting law enforcement to develop AI-powered tools that assist in the recovery of the proceeds of crime, including from fraud**, and improve intelligence sharing. These capabilities will help Financial Investigators complete orders more efficiently, assist officers responding to intelligence requests, and enhance collaboration within the UK and with international law enforcement partners. By streamlining investigative processes and civil remedies, AI will strengthen efforts to deprive criminals of illicit gains.

111. Accurate data and performance metrics underpin effective leadership and response. **The Home Office will therefore review and improve how fraud offences and outcomes are recorded in the Home Office Counting Rules,** modernising and streamlining categories, and aligning with other official datasets. This will make it easier for forces to manage cases, measure performance and target interventions. In parallel, wider performance of local forces and regional forces will be **reviewed through His Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) Police Effectiveness, Efficiency and Legitimacy (PEEL) inspection framework**, improving consistency and standards for investigations and victim care.

112. An effective law enforcement response relies on skilled people as well as strong structures. By 2028, **the Home Office will implement recommendations from the Police Skills Review** with the City of London Police's Economic and Cyber Crime Academy (ECCA) and the College of Policing. This includes a clear training framework, a skills gap analysis, and new courses to upskill officers in fraud, cyber, and economic crime. Training will also cover victim support and public fraud prevention. The ECCA's Fraud and Economic Crime app will support these initiatives by providing quick access to guidance, tools, and resources.

113. Retention of expertise is equally critical. Building on the skills review and the Workforce Strategy for Economic Crime, **the Home Office will work with law enforcement and industry to design and deliver an economic crime 'profession'** by 2029. This will establish career pathways and skills frameworks to help specialists develop and remain in role, aligning with existing counter-fraud professions such as that delivered by the Public Sector Fraud Authority. These measures will deepen expertise across law enforcement and provide a clear offer to retain trained and talented staff.

114. As criminals target businesses with increasingly sophisticated schemes, law enforcement must develop sector-specific expertise. Many business-related fraud cases are complex and often go unreported. To address this, **the Home Office will develop proposals for new business-funded units in the most affected sectors**, with the aim that the first unit will be fully operational in 2028/9. These units will specialise in fraud affecting businesses, providing additional capacity and expertise, and will build on proven models such as the Dedicated Card and Payment Crime Unit (DCPCU), the Insurance Fraud Enforcement Department (IFED), and the Police Intellectual Property Crime Unit (PIPCU). The initial focus will be on the retail sector, which has been particularly impacted by customer fraud and impersonation.

115. A specialist approach is also needed for fraud targeting the most vulnerable. Trading Standards reports that vulnerable individuals receive up to six times more fraudulent calls and texts, and some victims documented by criminals receive up to 70 fraudulent letters a day.[88] These crimes are often orchestrated from abroad but facilitated within the UK. To combat this, in 2026 Government will **pilot a new joint Trading Standards and law enforcement unit** to harness Trading Standards' civil and consumer powers to disrupt high-volume fraud and to recover assets from criminals.

6.3 International law enforcement collaboration

Fraud is not confined by borders. Criminals exploit global networks, digital platforms, and cross-jurisdictional vulnerabilities to target UK citizens and businesses from overseas and often out of reach of UK law enforcement. Responding to this challenge requires law enforcement collaboration across borders that is as agile and interconnected as the threat itself.

116. The Government is committed to leading the international fight against fraud, ensuring criminals face justice wherever they operate and deterring future offences. Central to this is a network of strategic partnerships. UK law enforcement will continue to **work bilaterally and multilaterally with allies, leveraging International Liaison Officers and collaborating with INTERPOL and Europol to share intelligence and conduct joint operations, and coordinate disruption**. Effective data sharing is key to tackling organised criminal gangs, and the Home Office and National Economic Crime Centre will work with partner countries to review legal frameworks and remove barriers to cross-border intelligence exchange, enabling greater policy alignment and operational cooperation.

Case Study: Operation SERENGETI 2.0

Operation Serengeti 2.0 was a UK-supported, INTERPOL-coordinated operation which resulted in the arrest of over 1,200 criminals across Africa, targeting nearly 88,000 victims and the recovery of USD 97.4m.

The operation involved investigators from the UK and 18 African countries to tackle high-harm, high-impact crimes including investment fraud, business email compromise and ransomware. Private sector partners strengthened the operation by providing intelligence, guidance and training to help investigators act on intelligence and effectively identify offenders.

117. INTERPOL will remain a vital partner, including through its ALERT system for tracing assets and individuals linked to crime. The UK will strengthen engagement across INTERPOL’s economic and cyber crime programmes and contribute expertise to global operations such as Operation Serengeti. We will also work with Europol to maximise UK reach, with proactive intelligence exchange through Europol’s SIENA and participation in multidisciplinary initiatives.

118. The UK will further **support INTERPOL in establishing a Global Fraud Taskforce** by 2029 to coordinate international investigations and dismantle criminal operations including scam compounds. The Taskforce will focus on three pillars: tactical enforcement (arrests, asset seizures), strategic disruption (sanctions, supply chain interference, travel restrictions), and public-private partnerships to address industry enablers.

6.4 Delivering justice through criminal and civil outcomes

Delivering justice is essential to victims' recovery, minimising repeat offending, and ensuring criminals are punished. Traditional criminal enforcement has a key role to play, especially in responding to the highest harm frauds. However, in many cases, where there is not enough evidence for prosecution, civil action will be more effective in responding at pace to high volume fraud.

119. In the year ending September 2025, only 3,631 individuals ultimately received a sentence. Faced with this scale of offending, a new approach is required which both enhances our criminal justice approach and leverages civil justice for lower-level offending.[89]

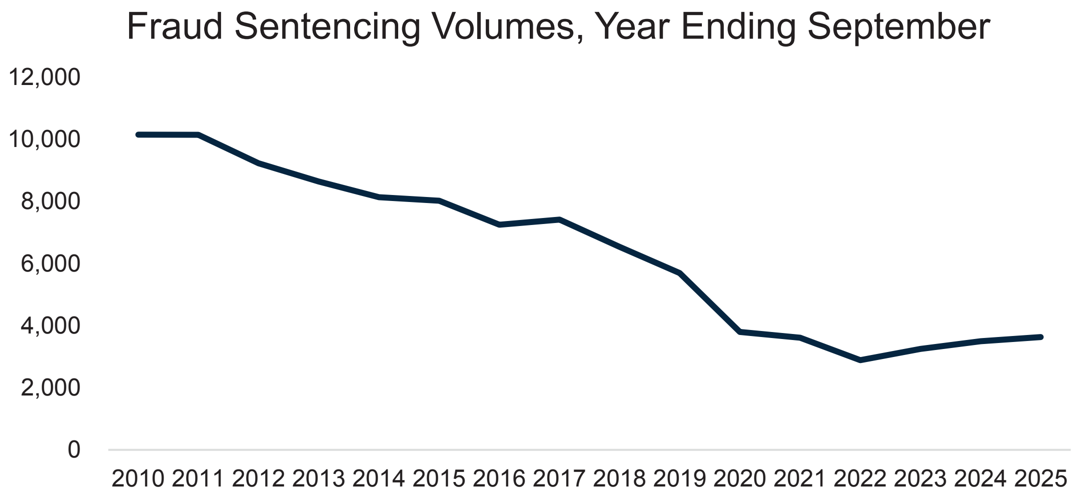


Figure 3: Annual offenders sentenced for fraud, year ending September 2010 to year ending September 2025 (NFIB codes 51, 52, 53.4, 53.6, 53B.1, 53C, 53D, 53E, 53F) Source: MOJ Criminal Justice Statistics year ending September 2025.

120. To deepen our understanding of the evolving fraud threat, and to ensure our legislative framework remains fit for purpose, the Government commissioned Jonathan Fisher KC to undertake an independent review of the barriers to detecting, investigating and prosecuting fraud. Having now received his report, **the Government will carefully consider its findings and recommendations**, which will help shape a more adaptive, agile and future-focused response to the changing methods and scale of fraud.

121. Delivering justice in fraud cases is increasingly challenging, in part due to the complexity of evidence. While the proportion of prosecutions resulting in convictions has remained broadly stable at an average of 82% over the past 5 years, the

number of fraud cases being prosecuted overall has fallen 56% since 2015.[90] To ensure faster resolution and avoid delays in bringing serious offenders to justice, as announced on 2 December, the **Government will introduce judge-only trials for the most complex fraud cases** by the end of this Parliament.[91]

122. Additionally, rising volumes of digital evidence and outdated legislation further strain resources, with fraud cases now taking over 626 days to reach charge compared to 80 days for the average case. [92,93] The **Government is therefore committed to modernising disclosure so that it is fit for purpose in the digital age**, as set out in the Written Ministerial Statement on 26 January 2026, to cut red tape and harness AI responsibly to streamline investigations and free up millions of police hours.[94,95]

123. To prevent recidivism among serious offenders, the Border Security, Asylum and Immigration Act 2025 strengthens the Serious Crime Prevention Order (SCPO) regime by expanding the range of bodies that can apply directly to the High Court (including the NCA, police forces, British Transport Police, MOD Police and HMRC), confirming the court's express power to impose electronic monitoring with specified safeguards and time limits, standardising notification requirements for SCPO subjects, and empowering the Crown Court to make an SCPO on acquittal or following appeal.

124. Civil enforcement will complement criminal sanctions. **The Home Office is supporting law enforcement pilots focused on pursuing legal action against criminals** and recovering money for victims through civil law by 2028. As set out in the July 2025 response to the Lords Liaison Committee, **the Home Office will also continue to consider whether introducing civil penalties for fraud and facilitating money laundering** will produce an effective alternative to the criminal law.[96] This will potentially draw on models such as the Public Authorities (Fraud, Error and Recovery) Act 2025, giving powers to issue civil penalties for fraud and attempted frauds. [97]

Case Study – Civil Recovery (private communication)

An online retailer brought 590 successful civil claims against people who had committed returns fraud to obtain goods without paying. Of these, 438 cases have been resolved, with defendants having paid a total of £271,000. The remaining 154 successful cases, totalling just under £100,000, are on payment plans.

6.5 Summary of Respond actions

125. **Improving Victims' Experiences:**

- Government will work with City of London Police to embed and operate the new Report Fraud service (from 2026);
- The Home Office will introduce a Fraud Victims Charter (in 2027); and
- The Home Office will explore opportunities to further support fraud victims with identity repair.

126. **Enhancing law enforcement investigative capabilities:**

- The Home Office will deliver the impact evaluation of the National Fraud Squad (in 2027);
- The Home Office will work with Ofcom and industry to implement a national telecommunications traceback scheme (by early 2028);
- Government will support law enforcement to develop AI-powered tools that assist in the recovery of the proceeds of crime, including from fraud;
- The Home Office will review and improve how fraud offences and outcomes are recorded in the Home Office Counting Rules (in 2027);
- Government will review the local police response through the HMICFRS PEEL inspection framework;
- The Home Office will implement the recommendations of the police skills review (by 2028);
- The Home Office will design and deliver an economic crime 'profession' (by 2029);
- The Home Office will develop proposals for new business funded units (in 2028); and
- The Home Office will pilot a new joint Trading Standards and law enforcement unit (in 2026).

127. **International law enforcement collaboration:**

- The Home Office will work with INTERPOL and Europol to conduct joint operations and share intelligence; and

- The Home Office will support INTERPOL to establish a Global Fraud Taskforce (by 2029).

128. **Delivering justice through criminal and civil justice outcomes:**

- Government will consider the proposals from the Independent Review of Fraud;
- Government will introduce judge-only trials for the most complex of fraud cases (by the end of this Parliament);
- Government is committed to modernising disclosure so that it is fit for purpose in the digital age;
- The Home Office will support law enforcement pilots of civil powers to pursue criminals and recover money for victims (by 2028); and
- The Home Office will consider introducing civil penalties for fraud and money laundering.

7. Governance and Accountability

The scale and sophistication of fraud, and the complexity of the system which seeks to combat it, demand a robust governance framework underpinned by accountability, coherence and insight. Through an enhanced governance structure, we will ensure clear leadership to drive the implementation of the Fraud Strategy, evaluate impact, and hold the counter-fraud system to account.

7.1 Leadership and governance

129. This Strategy establishes a strengthened governance model which provides clarity on roles and responsibilities and increases oversight of delivery. The Home Office will embed systemic risk management throughout the counter-fraud system and governance, improving our ability to anticipate and respond to evolving threats, make informed decisions, and maintain resilience.

130. Strong Ministerial oversight is essential to ensure that fraud remains a national priority. The Home Secretary holds overall responsibility for tackling fraud against individuals and businesses, supported by the Home Office Minister of State responsible for tackling fraud, who leads day-to-day delivery and cross-system engagement.

131. The Economic Crime Strategic Board (ECSB) will retain of the Governments response to economic crime, including fraud. Beneath the ECSB sits the Joint Fraud Taskforce (JFT) and the new Ministerial Accountability Group.

132. The JFT will continue to meet quarterly and bring together Ministers from relevant Government departments, law enforcement, regulators, and industry to coordinate action and monitor progress. The JFT will continue to represent the highest tier of the public-private partnership within the counter-fraud system.

133. Successful delivery of this Strategy will also include ensuring strong oversight of delivery and performance of the full range of the public sector organisations involved in tackling fraud. We are therefore **introducing a new Fraud Ministerial Accountability Group,** to be chaired by the Home Office Minister of State with responsibility for tackling fraud, which will sit alongside the JFT to provide a single cross-public sector function for strategic decision-making and accountability at the highest level.

134. An annual report will also be provided to Ministers on progress to ensure strategic direction is regularly reviewed and the counter-fraud system is held to account.

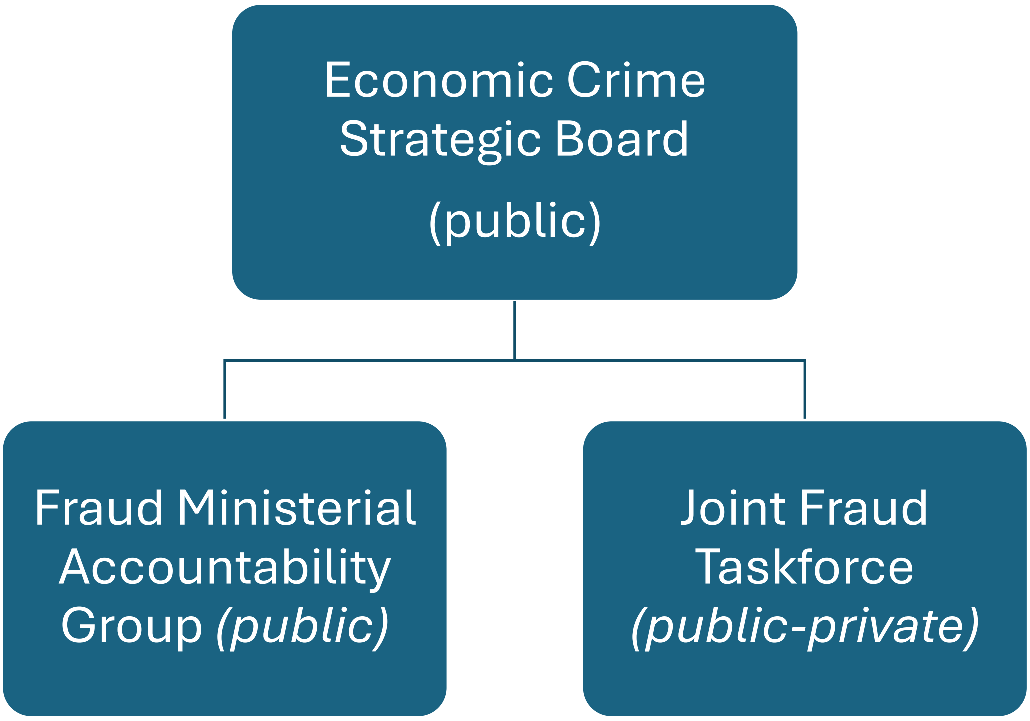

Economic Crime Strategic Board (public)
Fraud Ministerial Accountability Group *(public)*
Joint Fraud Taskforce *(public-private)*

Figure 4: Fraud Strategy governance structure

7.2 Strategic coherence

135. Fraud does not exist in isolation. This Fraud Strategy is embedded within a broader ecosystem of national strategies which set direction on protecting the UK's people and businesses from a range of interlinked security and SOC threats. The Home Office has worked closely with the owners of each of these strategies to ensure that the proposed activity is aligned. This includes the 2025 National Security Strategy, Economic Crime Plan 2, Anti-Corruption Strategy, forthcoming National Cyber, Cyber Crime, and Anti-Money Laundering and Asset Recovery Strategies, as well as the 2024-2027 Counter Fraud Functional Strategy which focuses on public sector fraud.

136. There will be increased alignment between the efforts to tackle fraud and the work to tackle cyber crime. The pace of technological change and the highly sophisticated nature of modern fraud criminality means that many if not most frauds are enabled by volume cyber crime. We will continue to work towards closer alignment of policy, delivery and governance as the fraud and cyber crime systems evolve.

137. Law enforcement remains operationally independent, but in a system as complex as this one, it is essential that strategy and operations are aligned. The refreshed governance model will therefore align priorities across threat areas, ensuring strategic coherence and consistent accountability for performance.

7.3 Metrics

138. To maintain oversight of the Strategy, we will review an expanded suite of indicators (Annex B) to provide a more comprehensive and nuanced picture of the Strategy's impact, enabling us to measure progress across multiple dimensions of the fraud landscape. This builds on the foundations established by the Economic Crime Plan 2 Outcomes Progress Report and the previous Fraud Strategy, ensuring continuity while incorporating new data sources and methodologies to improve accuracy and relevance.[98,99]

139. Fraud statistics are measured through the Crime Survey for England and Wales (CSEW) for individuals and the Economic Crime Survey (ECS) for businesses with employees. Estimates from CSEW, updated quarterly, capture both reported and unreported incidents and are not influenced by changes in reporting behaviour or public awareness. Evidence from the ECS 2024 has been added as it provides evidence on the number of incidents, and number of victims of fraud who are businesses. **The Home Office will continue to track trends through a survey of businesses' experience of fraud**. The Home Office will continue working with delivery partners to strengthen available data and further refine this framework, including developing a theory of change, advancing data improvement efforts, and identifying priority areas for in-depth evaluation.

140. The Home Office will publish an update outlining key insights on delivery progress, as well as developments in new data that address current limitations and strengthen our ability to measure performance comprehensively. The intention is for this to be completed once during the Strategy delivery period, and again after the end of this period. Engagement will continue with delivery partners to strengthen data and to develop the outcomes framework and associated metrics over the course of the strategy.

7.4 Delivery partners

Departments and Non-Departmental Public Bodies

Cabinet Office: The Cabinet Office leads the UK’s cross-Government approach to countering fraud in the public sector. It sets the strategic direction, develops mandatory standards (such as GovS 013), and oversees the Government Counter Fraud Function. Through the Public Sector Fraud Authority, it drives professionalisation, capability building, and innovation, ensuring departments and public bodies work together to prevent, detect, and respond to fraud. It is also leading the development of the new national Digital ID Scheme.

Charity Commission: The Charity Commission for England and Wales is the regulator of charities in England and Wales. It is an independent, non-ministerial government department accountable to Parliament. As registrar, the Commission is responsible for maintaining an accurate and up-to-date register of charities. This includes deciding whether organisations are charitable and should be registered. The Commission also removes charities that are not considered to be charitable, no longer exist or do not operate. The Office of the Scottish Charity Regulator and the Charity Commission for Northern Ireland are the regulators in Scotland and Northern Ireland respectively.

Companies House: Companies House is the official registrar of companies in the UK. It is responsible for incorporating and dissolving companies, maintaining an up-to-date register of company information, and ensuring compliance with UK company law. Companies House provides access to public information about companies, including registered addresses, details of directors and shareholders, and annual financial filings, promoting transparency and accountability in the UK economy. The Economic Crime and Corporate Transparency Act (2023) introduced significant reforms to Companies House to improve transparency, strengthen the UK’s business environment, support national security and disrupt economic crime.

Crown Prosecution Service (CPS): The CPS is responsible for prosecuting criminal cases, including fraud, that were investigated by the police and other agencies in England and Wales. The CPS provides legal advice during investigations, makes charging decisions, and presents cases in court, working closely with law enforcement and regulatory bodies to bring criminals to justice.

Department for Business and Trade (DBT): DBT plays a key role in protecting the integrity of the UK's business environment. It develops policy and regulation to prevent fraud in business, supports companies in managing fraud risks, and works with partners to tackle economic crime, including fraud affecting trade and commerce.

Department for Culture, Media and Sport (DCMS): DCMS is responsible for media and creative industries policy, which includes advertising. It is also the lead department for the Online Advertising Taskforce, which is chaired by the Minister for Creative Industries, Media and Arts.

Department for Education (DfE): DfE plays a key role in safeguarding children and young people, including supporting schools to educate young people on media literacy, online harms and financial education.

Department for Science, Innovation and Technology (DSIT): DSIT is responsible for policy on the online ecosystem, digital identity and telecommunications, as well as leading on AI policy. It is responsible for online and telecommunications legislation. The Office for Digital Identity and Attributes (OfDIA) sits within DSIT. DSIT also acts as the sponsoring department responsible for managing the relationship between the Government and Ofcom, in relation to Ofcom's functions, duties, and powers.

Financial Conduct Authority (FCA): The FCA regulates financial services firms and markets in the UK. It sets standards to prevent and detect fraud in the financial sector, supervises firms' counter-fraud controls, and takes enforcement action against those who commit or facilitate fraud. The FCA also works with law enforcement and international partners to disrupt financial crime.

Foreign, Commonwealth and Development Office (FCDO): The FCDO leads the UK's international engagement and supports HMG capability when working overseas to engage other Governments, international organisations, and law enforcement partners to tackle cross-border fraud. The FCDO also has responsibility for HMG sanctions policy.

HM Courts and Tribunals Service (HMCTS): HMCTS administers the justice system in England and Wales, supporting the prosecution and adjudication of fraud cases. It ensures that courts and tribunals are equipped to handle complex fraud trials and supports the recovery of assets from convicted criminals.

HM Treasury (HMT): HMT is responsible for the overall management of public finances and oversees financial services policy.

Home Office: The Home Office reduces homeland security risks to the UK's people, prosperity and freedoms through the Homeland Security Group (HSG). This includes the risks from fraud and wider economic crime. It provides systems leadership across Government and delivers strategic initiatives, working closely with law enforcement, regulators and other external organisations to develop policy, strengthen legislation and support operational activity to prevent and disrupt fraud and protect the UK. The Home Secretary has overall responsibility for fraud against individuals and businesses, with the dedicated Minister for Fraud leading on day-to-day delivery.

Insolvency Service: The Insolvency Service is an executive agency of the Department for Business and Trade. Its primary responsibilities include administering bankruptcies and company liquidations, investigating financial misconduct, enforcing regulations, providing information on insolvency processes and administering redundancy payments when companies become insolvent. Following The Economic Crime and Corporate Transparency Act 2023 the Insolvency Service is expanding its enforcement role.

Ministry of Housing, Communities and Local Government (MHCLG): MHCLG supports local authorities in managing fraud risks in local Government services.

Ministry of Justice (MoJ): The MOJ oversees criminal justice policy and the justice system, including the prosecution and punishment of fraud offences, as well as the detention and rehabilitation of offenders. It works with HMCTS, the CPS, and law enforcement to ensure that fraud cases are effectively managed through the courts and that victims receive appropriate support.

Office of Communications (Ofcom): Ofcom regulates the UK's communications sectors, including telecommunications and online platforms such as social media and search engines. It works with industry to prevent and disrupt fraud, such as spoof calls and online fraud, and supports public awareness initiatives to help consumers protect themselves.

Payment Systems Regulator (PSR): The PSR ensures payment systems are fair, efficient, and secure, with a strong focus on protecting consumers from fraud. Its role includes setting rules that require payment service providers to implement effective fraud prevention measures and monitoring practices. A key responsibility is enforcing reimbursement requirements for victims of certain types of fraud.

The Pensions Regulator: The Pensions Regulator is the public body responsible for protecting workplace pensions in the UK. It ensures that employers, trustees, and pension specialists fulfil their duties to scheme members, and it sets out guidelines to ensure the security of savers' money. TPR heads the Pension Scams Action Group (PSAG), a multi-agency taskforce of law enforcement, government and industry working together to tackle pension fraud.

Public Sector Fraud Authority (PSFA): The PSFAis the centre of expertise for countering fraud in the public sector. It leads on strategy, capability building, and innovation, provides guidance and support to departments and public bodies, and drives the use of data and technology to detect and prevent fraud.

Serious Fraud Office (SFO): The SFO investigates and prosecutes serious or complex fraud, bribery, and corruption. It handles cases of national importance or involve significant public interest, working closely with domestic and international partners.

Law Enforcement and Intelligence Partners

City of London Police (CoLP): CoLP has specialist expertise on tackling fraud, including raising awareness, monitoring performance, sharing intelligence, promoting best practice, and providing training and peer support. This includes supporting forces with implementing the National Policing Strategy for Fraud, Economic and Cyber Crime 2023-2028 and providing operational training through their Economic and Cyber crime academy. CoLP manage Report Fraud, the new national reporting service for fraud, which analyses reports and disseminates viable cases to police forces. CoLP additionally manages the Report Fraud Victim Services, and the national coordination function of the Fraud Protect Coordinators Network, to deliver targeted crime prevention messaging to help the public protect themselves by increasing their resilience to fraud. Subject to the findings of the Independent Review of the Police Force Structures, we will assess whether CoLP's specialist services should transfer to the NPS or could be delegated and continue to be delivered by the City of London Police under NPS direction.

College of Policing: The College of Policing sets professional standards and provides training for police officers and staff, including in the investigation and prevention of fraud. It develops guidance and supports continuous improvement in policing practice.

Local Police Forces in England and Wales: The 43 territorial police forces in England and Wales are responsible for investigating fraud offences and supporting victims in their areas, supported by national capabilities, coordination and leadership offered through the City of London Police and the NCA. They also play a key role in raising awareness and building local resilience against fraud.

National Police Service (NPS): The NPS will provide a single source of strategic leadership for the police service, replacing the confused mix of existing institutions. It will set stronger national standards, to ensure a more consistent service for the public across the country. The NPS will also provide local policing with better enabling and support services such as national IT, national commercial, and forensics. The NPS will additionally strengthen our ability to tackle terrorism and serious and organised crime by bringing together the National Crime Agency (NCA), Counter Terrorism Policing (CTP) and Regional Organised Crime Units (ROCU). Overall responsibility for Fraud, Economic Crime and Cyber Crime will transfer to the NPS with the NCA, and the NPS will be the lead agency for these crimes. This will ensure a more streamlined approach with clearer roles and more effective tasking responsibilities.

National Crime Agency (NCA): The NCA leads the UK’s fight against serious and organised crime, including complex and high-value fraud. It coordinates national and international investigations, disrupts criminal networks, and works with partners to recover criminal assets. As above, the NCA will transfer to the NPS.

National Economic Crime Centre (NECC): The NECC, hosted by the NCA, brings together law enforcement, regulators, and Government to coordinate the UK Law Enforcement response to economic crime, including fraud. It sets priorities, shares intelligence, and leads joint operations to tackle the most serious threats. The NECC provides operational system leadership to the fraud system response. This includes engagement with industry through several public-private partnership models and with international law enforcement partners to protect UK citizens from fraud originating overseas. The NECC also provides leadership (jointly with the City of London Police) to the National Fraud Squad of specialist fraud investigators which uses intelligence to proactively identify and disrupt the most serious criminals targeting the UK.

National Trading Standards (NTS): NTS are local council departments in the UK responsible for ensuring fair trading, consumer protection, and compliance with laws related to product safety and business practices. NTS operates in England and Wales and is responsible for gathering important intelligence to combat rogue traders. NTS also has teams that focus on combatting large scale fraud and e-crime across England and Wales. Trading Standards Scotland and The Northern Ireland Trading Standards Service operate in Scotland and NI respectively.

Regional Organised Crime Units (ROCUs): ROCUs provide specialist support to police forces in tackling serious and organised crime, including fraud. They deliver intelligence, investigation, and disruption capabilities at a regional level, bridging the gap between local and national efforts.

Police Scotland: Police Scotland leads the response to fraud across Scotland, investigating offences, supporting victims, and working with partners to prevent harm. They contribute to national coordination through engagement with UK-wide initiatives and share intelligence to tackle cross-border fraud threats.

Police Service of Northern Ireland (PSNI): PSNI is responsible for investigating fraud offences in Northern Ireland and supporting victims locally. They work closely with UK law enforcement partners to share intelligence and coordinate responses to fraud that impacts communities across jurisdictions.

UK Intelligence Community (UKIC): Led by GCHQ, UKIC will continue to utilise its unique capabilities to understand the evolving threat of fraud and its strategic enablers, to provide delivery partners with intervention opportunities, thereby disrupting the associated international organised crime and protecting UK citizens from fraud and cyber crime.

Private Sector Partners

Financial Services Sector: The financial services sector plays a vital critical role in preventing, detecting, and disrupting fraud. Firms work with law enforcement agencies, regulators and Government to share intelligence, enhance customer protections, and implement measures to reduce fraud risk across banking, payments, and investment services.

Telecommunications Sector: Telecommunications providers help prevent fraud by securing communication channels and reducing opportunities for criminals to exploit phone and messaging services. They collaborate with Government and law enforcement to block fraudulent calls and texts and share data to identify emerging threats.

Technology Sector: Technology companies are key partners in tackling online fraud. They work to protect users by improving platform security, removing fraudulent content, and sharing intelligence on criminal activity. Collaboration with law enforcement and Government helps ensure rapid responses to new and evolving fraud methods.

The Public, Civil Society, and Non-Governmental Organisations

Civil society groups, NGOs, and academic institutions contribute expertise, research, and advocacy to the UK’s counter-fraud efforts. They support victims, raise public awareness, and provide independent scrutiny of Government and industry action. Academia also drives innovation in fraud detection and prevention through research and collaboration.

8. Annexes

Annex A: Delivery plan

DISRUPT						
Action	**Delivery Lead/ Partners**	**Delivery Commence/ Complete Date**		**Action**	**Delivery Lead/ Partners**	**Delivery Commence/ Complete Date**
Launch the Online Crime Centre	Home Office NCA, CoLP Online, Telecommunications and Financial sectors	Commence Q1 2026		Industry partnership under Online Advertising Taskforce report	Home Office DCMS Online Industry	Complete Q1 2027
Launch a Call for Evidence to identify barriers to data sharing	Home Office	Commence Q1 2026		Monitor and evaluate regulations and enforcement powers in online marketplaces	DBT DCMS Ofcom	Ongoing
Support law enforcement to leverage emerging technologies	Home Office NCA	Ongoing		Improve the security of AI models	Home Office DSIT	Ongoing
Sponsor the Global Fraud Summit in Vienna in March 2026	Home Office UNODC INTERPOL NCA	Complete Q1 2026		Launch a Call for Evidence on unauthorised fraud	Home Office	Commence Q4 2026
Pursue MoUs and bilateral partnerships with high priority countries	Home Office FCDO NCA	Ongoing		The FCA will share best practice recommendations in relation to APP fraud and exploitative money laundering	FCA	Ongoing

Action	Delivery Lead/ Partners	Delivery Date		Action	Delivery Lead/ Partners	Delivery Date
Continue use of sanctions against malign actors overseas	FCDO	Ongoing		HMT repeal the existing Strong Customer Authentication (SCA) technical standards	HMT	As soon as parliamentary time allows
Oversee the implementation of the second Telecommunications Fraud Charter	Home Office Telecommunications sector	Complete Q4 2027		Accelerate the adoption of passkeys	National Cyber Security Centre (NCSC)	Ongoing
Launch a Call for Evidence for reducing anonymity and strengthening accountability in the communications sector	Home Office Ofcom	Commence Q2 2026		Regulate cryptoasset financial services activities	HMT FCA	The FCA will finalise its rules in 2026, ahead of the regulatory regime coming into force in October 2027
Develop options to create a secure digital tool to manage UK telephone numbers.	Home Office	Conclude Q4 2026		Set up an anti-phoenixism taskforce within the Insolvency Service to tackle abusive company phoenixism	Insolvency Service	Commence Q2 2026
Develop data sources and metrics to track industry performance in tackling fraud	Home Office Online, Telecommunications and Financial Services sectors	Ongoing		Mandate electronic invoicing for all VAT invoices from April 2029	HMRC	Roadmap Q4 2026 Implementation Q2 2029
Introduce the Fraudulent Advertising Duty	Ofcom	Complete Q4 2027		Consider digital company identities as a way to secure electronic identities and streamline verification of transactions	DBT	Ongoing

SAFEGUARD						
Action	**Delivery Lead/ Partners**	**Delivery Commence/ Complete Date**		**Action**	**Delivery Lead/ Partners**	**Delivery Commence/ Complete Date**
Expand Stop! Think Fraud campaign	Home Office	Commence Q2 2026		Upscale use of PROTECT Network Volunteers	CoLP	Commence Q2 2026
Develop impartial and comprehensive consumer advice	Home Office	Complete Q4 2026		Improve how the PROTECT Network responds to notifications from industry	CoLP	Commence Q2 2026
Embed educational resources for school children in England	SWROCU PSHE	Commence Q4 2026		Launching a Financial Safeguarding Scheme	Home Office	Commence Q2 2026
Increase resilience to fraud within university students	Home Office CoLP	Commence Q3 2026		Fund National Trading Standards scams team to support multi agency approach to fraud	Home Office NTS	Commence Q2 2026
Develop a system-wide response to protect individuals at risk of abuse of position	Home Office Law enforcement	Commence Q2 2026		FCA will conduct analysis of ‘cashing-out’ and work with industry to tackle money laundering.	FCA	Ongoing
Support for cyber resilience centres	Home Office CoLP	Ongoing		The Home Office will work with the Children’s Society to expand support for children at risk of financial exploitation	Home Office The Children’s Society	Commence Q3 2026

Action	Delivery Lead/ Partners	Delivery Commence/ Complete Date		Action	Delivery Lead/ Partners	Delivery Commence/ Complete Date
Increase intelligence led PROTECT activity in local areas	Home Office CoLP	Commence Q3 2026		Strengthen national coordination of fraud prevent activity	CoLP	Commence Q2 2026
Align the Fraud & Cyber PROTECT Network	CoLP	Commence Q2 2026				

RESPOND						
Action	**Delivery Lead/ Partners**	**Delivery Commence/ Complete Date**		**Action**	**Delivery Lead/ Partners**	**Delivery Commence/ Complete Date**
Embed and operate new Report Fraud Service	Home Office CoLP	Commence Q1 2026		Design and deliver an economic crime ‘profession’	Home Office	Complete Q4 2028
Introduce a Fraud Victims Charter	HO CoLP	Complete Q4 2027		Develop proposals for new business-funded sector units	Home Office Sectors	Complete Q3 2028
Explore opportunities to further support fraud victims with identity repair	Home Office	Ongoing		Pilot a new Joint Trading Standards and law enforcement unit using NTS civil powers	Home Office NTS	Commence Q2 2026
Conduct an impact assessment of the National Fraud Squad (NFS)	Home Office	Complete Q4 2027		Conduct joint operations and share intelligence with INTERPOL and Europol	Home Office NCA INTERPOL Europol	Ongoing
Implement a National Telecommunications Traceback Scheme	Home Office Telecommunications sector	Complete Q2 2028		Support INTERPOL to establish a Global Taskforce	Home Office NCA INTERPOL Europol	Complete Q3 2028
Supporting law enforcement to develop AI-powered tools that assist in the recovery of the proceeds of crime, including from fraud	Home Office Law enforcement	Ongoing		Government will consider the proposals from the Independent Review of Fraud	Home Office	Ongoing
Improve Home Office Counting Rules for fraud	Home Office CoLP	Complete Q4 2027		Continue to support the law enforcement pilots focused on pursuing legal action against criminals and recovering money for victims through civil law	Home Office CoLP	Complete Q4 2027

Action	Delivery Lead/ Partners	Delivery Commence/ Complete Date
Review the local police response through HMICRS PEEL inspection framework	Home Office	Ongoing
Implement the recommendations of the police skills review	Home Office	Complete Q4 2027

Action	Delivery Lead/ Partners	Delivery Commence/ Complete Date
Consider introducing civil penalties for fraud and facilitating money laundering	Home Office MoJ	Ongoing

Annex B: Metrics

Headline Metrics	
CSEW and ECS Fraud Incidents	4.15 million incidents against individuals in year-end (YE) September 2025, an 8% increase on YE September 2024 (not statistically significant).[100] Estimated 6.04 million incidents against businesses with employees in the twelve months prior to the survey (ECS 2024).[101,102]
CSEW Proportion of all crime	Fraud accounts for 45% of all crime in YE September 2025, up from 41% in YE September 2024.[103]
CSEW Victim Prevalence	3.6 million adult victims (7.3%), 1 in 14, in YE September 2025, an 11% increase on YE September 2024.[104]
UKFI Average losses	£318 average loss for authorised and unauthorised fraud in YE June 2025, down 11% from YE June 2024.[105]
Report Fraud reported losses	£3.5 billion in reported fraud losses to Action Fraud (YE October 2025), an average of £10,300 per report. This cannot currently be compared to previous years.[106]
CSEW Incidents without loss	25% of fraud incidents resulted in no financial loss, a 1 percentage-point decrease from YE September 2024.[107]
UK Finance APP reports	222,000 APP fraud cases in YE June 2025, 6% decrease from YE June 2024.[108]
Number and proportion of Report Fraud high harm fraud type reports[109]	21% of total Action Fraud reports were high harm fraud reports (67 thousand) in YE September 2025.[110]
Number of law enforcement disruptions	2,862 system-wide disruptions in YE March 2024[111], a 54% increase on the previous year.

Annex C: Stakeholder engagement summary

1. The development of this Fraud Strategy was underpinned by extensive engagement with a broad spectrum of stakeholders. These included industry leaders, law enforcement agencies, academic experts, and civil society organisations. This inclusive approach ensured the Strategy reflects diverse perspectives and is grounded in real-world experience and insights.
2. The Home Office led a comprehensive and iterative engagement process, hosting over fifty roundtables, bilateral meetings and reading rooms and receiving over sixty detailed written submissions containing over a thousand individual pieces of feedback. This collaborative effort enabled stakeholders to actively shape, critique, and refine the core elements of the Strategy, ensuring it is both evidence-based and has secured broad support.
3. The Government is grateful to all individuals and organisations who contributed their time, expertise, and feedback. Their commitment to working in partnership with Government has been instrumental in shaping a robust, forward-looking Strategy to tackle fraud at scale. Core themes included:

Data sharing and disruption

4. **Data fragmentation & sharing barriers:** Tackling fraud is hindered by a data landscape lacking in standardisation, real-time sharing, as well as significant legislative, cultural, and technical barriers to effective data exchange.
5. **Proactive, upstream prevention:** Tackling fraud requires a shift toward upstream interventions such as real-time detection and targeting enablers of fraud rather than relying on reactive responses.
6. **Disruption-first strategy:** Long-term resilience depends on prioritising fraud prevention over post-fraud criminal justice and recovery, with strategic focus and resources directed at stopping fraud before it occurs.

Victims and vulnerability

7. **Early and inclusive fraud education:** Fighting fraud means embedding fraud awareness and financial literacy from a young age through the curriculum up to and including all age groups and potential vulnerabilities, supported by unified cross-sector messaging and behavioural interventions.

8. **Streamlined reporting & victim care:** This means improve fraud reporting through industry integration to reduce victim burden, while ensuring proactive, inclusive support regardless of fraud type or reimbursement status.
9. **Sector engagement & community mobilisation:** Encourage business reporting, deliver tailored sector-specific campaigns, and expand volunteer networks to strengthen fraud prevention efforts.

Justice outcomes

10. **Low confidence in justice outcomes:** Public trust in fraud reporting and policing is low due to limited prosecutions and weak deterrents; the focus should shift toward delivering meaningful justice beyond arrests.
11. **Enhanced investigative capabilities:** We need to strengthen digital investigation skills, use of technology and ensure a consistent police response to all fraud types.
12. **Broader use of civil powers:** Government should expand the toolkit for tackling fraud by leveraging civil sanctions and enforcement mechanisms alongside traditional criminal justice approaches.

Technology

13. **AI-driven threats & public vulnerability**: The rise of AI-powered fraud tactics, including deepfakes and spoofing, makes it harder for the public to detect fraud, demanding stronger industry incentives to disrupt these threats.
14. **Futureproofing strategy & technology:** The Fraud Strategy should consider emerging technologies, including stablecoins, blockchain, and new payment methods.
15. **Modernising investigations with AI:** Government should leverage AI and data to enhance digital investigative capabilities, ensuring law enforcement and industry are equipped to respond to increasingly sophisticated fraud techniques.

Global coordination

16. **Strengthen global coordination:** Government should advocate for enforceable international standards and deeper collaboration through alliances including Five Eyes the United Nations, and INTERPOL to enhance cross-border enforcement and intelligence sharing.

17. **System readiness & security by design:** Government needs to ensure UK systems are robust, and fraud prevention is embedded into new payment infrastructures before scaling international cooperation.
18. **Support for international enforcement:** Government should provide resources, training, and civil enforcement tools to empower global law enforcement in tackling transnational fraud effectively.

Annex D: Geographic scope

1. The legal framework for addressing fraud varies across the four nations of the UK. In England, Wales, and Northern Ireland, fraud is primarily prosecuted under the Fraud Act 2006. In contrast, Scotland treats fraud predominantly as a common law offence. It is important to note that policing and criminal justice are devolved matters in both Scotland and Northern Ireland, resulting in jurisdictional differences in how fraud is defined, investigated, and prosecuted.

2. The territorial extent of the National Police Service (NPS) will be UK-wide, but its powers and remit will vary between England and Wales, Scotland and Northern Ireland. In England and Wales, the NPS will have full operational powers and will be able to carry out its law enforcement activities and enabling services directly. In Scotland and Northern Ireland, the NPS will only be able to carry out operations with the agreement of the legally designated authority. This reflects the current arrangements for serious and organised crime and Counter Terror Policing in Scotland and Northern Ireland. NPS's location will be determined in due course. In addition to its national headquarters, NPS will have a regional footprint to exercise its functions at a regional level.

England and Wales

3. The City of London Police serves as the national lead force for fraud in England and Wales, overseeing the coordination of fraud reporting, victim care, and investigative efforts.

4. While fraud policy remains largely reserved in Wales, with limited devolution in this area, the Welsh Government continues to collaborate closely with the UK Government. This includes active participation in the Joint Fraud Taskforce (JFT) to support a unified approach to tackling fraud across the UK. It is important to note that education is a devolved matter in Wales, and the Welsh Government has responsibility for education policy and delivery. This distinction is relevant when considering fraud prevention and awareness initiatives, which may need to be tailored to reflect devolved competencies and ensure alignment with Welsh education frameworks.

Northern Ireland

5. In Northern Ireland, responsibility for policing and justice is devolved to the Department of Justice, which oversees criminal justice policy under the authority of the Northern

Ireland Assembly. The Police Service of Northern Ireland (PSNI) operates as the sole police force and leads on tackling serious and organised crime. It works closely in partnership with the NCA, HMRC, and other relevant bodies. The Public Prosecution Service for Northern Ireland (PPSNI) serves as the region's independent prosecuting authority.

6. The Organised Crime Task Force (OCTF) plays a central role in Northern Ireland's response to organised crime. It serves as a strategic forum that brings together law enforcement agencies, Government departments, and other key stakeholders to coordinate a collaborative and unified approach to tackling priority assessed areas organised crime, which includes certain types of fraud related activities.

7. In Northern Ireland, incidents of fraud and related cyber crime are typically reported to Report Fraud, or directly to the PSNI in specific circumstances. The region benefits from a well-established initiative known as the Scamwise NI Partnership, chaired by the PSNI, which brings together over 45 organisations united in their commitment to tackling fraud. The partnership includes a diverse range of stakeholders, such as youth organisations, charities, Government departments, law enforcement, and private sector representatives. Its work focuses on community awareness campaigns to educate the public about the risks and types of fraud, alongside information sharing to strengthen collective prevention efforts.

8. The Northern Ireland Cyber Security Centre provides cyber security guidance and advice to individuals and businesses and PSNI has PROTECT officers who work closely with the teams led by the City of London Police.

9. The Northern Ireland Department of Justice attends the JFT.

Scotland

10. In Scotland, the Crown Office and Procurator Fiscal Service (COPFS), operating under the authority of the Lord Advocate, is responsible for the investigation and prosecution of crime. Police Scotland serves as the national police service, leading on the investigation of economic crime in collaboration with agencies such as the NCA, HMRC, and the Financial Conduct Authority (FCA). Fraud is typically reported directly to Police Scotland, which holds primary responsibility for managing fraud investigations within the Scottish legal framework.

11. In March 2021, the Scottish Government published its Scams Prevention, Awareness and Enforcement Strategy, which provided a strategic framework to support both

protection and enforcement efforts. The Strategy aimed to reduce criminals' ability to operate and minimise the impact on victims when fraud occurs. To support this work, the Scottish Government established the Scottish Scams Strategic Partnership, which brought together a wide range of public and private sector organisations. The partnership promoted a unified voice and collective advocacy on key issues related to fraud prevention, public awareness, and enforcement. Its activities include public education campaigns and information sharing to strengthen Scotland's overall resilience to fraud. The work on the Strategy has now concluded.

12. The establishment of Consumer Scotland in 2022 means that Scotland now benefits from an independent public body which can provide leadership, take strategic oversight, and coordinate a fragmented consumer landscape. Consumer Scotland oversees the consumer advice and advocacy work of third sector organisations Citizens Advice Scotland and Advice Direct Scotland, both of which carry out fraud prevention and awareness work. Consumer Scotland has also provided funding to the Convention of Scottish Local Authorities for fraud prevention and awareness campaign work. Since April 2025, Consumer Scotland has been responsible for the strategic leadership of fraud prevention and awareness work across the consumer landscape.

13. In April 2025, Police Scotland merged several digital, cyber and serious organised crime teams to create a Cyber and Fraud Unit that will collaborate with other UK law enforcement partners and agencies to develop an effective response to the changing threat landscape. The unit will develop new capabilities to undertake proactive investigations, crime prevention, and protection for victims in the digital age. This will include investigative capability, use of cutting-edge technology, workforce training and support and guidance.

14. Police Scotland is also working closely with City of London Police to build the foundations that will enable Police Scotland to join the new Report Fraud service in the future.

15. The CyberScotland Partnership provides cyber resilience advice and guidance to Scotland's people, businesses and organisations and Police Scotland has PROTECT officers who work closely with the teams led by the City of London Police.

16. Scottish Government officials attend the JFT.

Annex E: Glossary

Advance fee fraud: A fraud where victims are persuaded to pay upfront fees for goods, services, or rewards that never materialise.

Authorised fraud / Authorised Push Payment (APP) fraud: Fraud where victims are deceived into authorising a payment to a criminal-controlled account.

Business email compromise: A type of fraud where criminals impersonate a trusted contact via email to divert payments or steal sensitive data from businesses.

Caller Line Identification: A feature that displays the caller's number, often spoofed by criminals to appear legitimate.

Carding: The illegal use or trading of stolen credit or debit card details to make fraudulent transactions.

Cloaking: A technique used by cybercriminals which hides the harmful nature or true destination of an advert/web link from scanning environments and security tools, only revealing the true harmful destination to potential victims. Cloaking differs from a traditional Traffic Distribution System (TDS) because cloaking hides a site's true destination by showing different content to different audiences, while a TDS simply routes users based on rules, without disguising the underlying content.

Communications routing: The process of directing calls or messages through telecommunications networks.

Company phoenixing: An abusive practice whereby directors close a company and reopen under a new name to evade debts or liabilities.

Competition and Markets Authority (CMA): A UK regulator that promotes competition and protects consumers from unfair business practices.

Computer software service fraud: A type of fraud where criminals pose as tech support workers to gain remote access to victims' devices or charge for fake services.

Courier fraud: A type of fraud where victims are deceived into handing over cash, cards or valuables to a criminal posing as a courier.

Cryptoassets: Digital representations of value or rights, including tokens such as Bitcoin or Ethereum and stablecoins, used for online transactions or investment. They rely on cryptography (a way of keeping data secure).

Customer authentication: Security processes that verify a user's identity before granting access or approving transactions.

Dark Web: Part of the internet intentionally concealed from standard web browsers and search engines (Google, Bing, Firefox etc.). Instead, specific dark web browsers are needed to access its content. This structure attempts to ensure the anonymity of users and website operators, protecting their identities and locations from being tracked.

Data breach: An incident where sensitive or personal data is accessed or disclosed without authorisation.

Deepfake: Synthetic media created using artificial intelligence to impersonate real people in audio, video, or images.

Exploitative money laundering: Coercing individuals who may often be children and young people or otherwise vulnerable, into laundering criminal proceeds.

Financial exploitation: Taking advantage of someone's vulnerability for personal financial gain, often through fraud.

Firewalls: Security systems that monitor and control network traffic to block unauthorised access.

Five Eyes (5EYES): An intelligence alliance between the UK, US, Canada, Australia, and New Zealand.

Frontier AI models: The most advanced AI systems with capabilities beyond current norms, posing new risks if misused.

Fungible cryptoassets: Digital tokens where every unit is the same and can be swapped for another without any difference in value. For example, one Bitcoin is worth the same as any other Bitcoin.

Generative artificial intelligence (GenAI): AI that creates new content (text, images, audio) based on patterns learned from data.

Grey web: Online spaces between the open internet and the dark web, providing goods or services which are illegal in most but not all jurisdictions. They are accessible using standard web browsers, but the websites themselves are not indexed on search engines, making them difficult to find unless the exact URL is known.

High harm fraud: Fraud types causing severe financial and emotional damage.

Hybrid romance-investment fraud: A type of fraud combining emotional manipulation with fake investment opportunities.

Hybrid threat: A threat spanning multiple vectors, such as cyber crime, state threats and fraud, to achieve criminal objectives.

Identity theft: The unauthorised use of someone's personal information to commit fraud or other crimes.

Investment fraud: Fraud where victims are misled into investing in fake or high-risk schemes.

Jurisdictions of risk: Countries or regions assessed as having high levels of fraud perpetrated from within their borders.

Large Language Models (LLMs): AI systems trained on vast text datasets to generate human-like language.

Lead generation: Collecting personal data for marketing or, in frauds, targeting victims.

Malware: Malicious software designed to damage systems or steal data.

Mass texting services: Platforms used to send bulk SMS messages; exploited for phishing.

Memorandum of Understanding (MOU): A formal agreement between parties, which could include Governments or other organisations, outlining cooperation without legal obligation.

Online-enabled fraud: Fraud facilitated or committed via the internet.

Online Safety Act Codes of Practice: The Codes of Practice set out measures recommended by Ofcom for service providers to comply with their safety duties and other duties specified under the Act.

Organised Crime Groups (OCGs): Structured criminal networks engaged in serious and organised crime, including fraud.

Passkeys: Cryptographic credentials that replace passwords for secure authentication.

Payment diversion fraud: Fraud where criminals redirect legitimate payments to their own accounts.

Payment Service Provider (PSP): A company that enables electronic payments for businesses and consumers.

Phishing: Fraudulent attempts to obtain money or data via emails, texts, or websites.

Purchase fraud: Where victims pay for goods or services that never arrive or do not exist.

Ransomware: Malware that encrypts data and demands payment for its release.

Romance fraud: Fraud where criminals exploit victims by posing as a romantic partner to build trust before manipulating them into sending money or personal data.

Scam compounds: Large-scale criminal operations housing individuals who may have been trafficked and forced to perpetrate fraud.

Scambaiting: Using decoy tactics to waste criminals' time and disrupt fraudulent operations.

Serious Crime Prevention Orders (SCPOs): Court orders restricting activities of individuals involved in serious crime.

Signals: Data indicators used to detect or disrupt fraud, e.g., suspicious IP addresses or phone numbers.

SIM swapping: Fraud where criminals impersonate their victim and request a new SIM (usually eSIM) from the mobile network operator to intercept calls and messages and gain access to the victim's log in details for online banking, emails and social media.

Smishing: Targets individuals thought fraudulent SMS messages.

Social engineering: Manipulating people into divulging confidential information or performing actions.

Spam filters: Tools that block unwanted or malicious emails or messages.

Spoofing: Falsifying telephone numbers to appear to be a legitimate caller or organisation.

Strategic Policing Requirement: A UK framework setting out national policing priorities for serious threats.

Traceback: A process to trace the origin of fraudulent calls through telecommunications networks.

Two-factor authentication: A security method requiring two forms of verification for access, which increases resilience to fraud.

Unauthorised fraud: Fraud where criminals access accounts or make payments without the victim's knowledge.

Virtual private network (VPN): A tool that encrypts internet traffic and masks location.

Voice cloning: AI-generated replication of a person’s voice used to impersonate them.

Voice over Internet Protocol (VoIP): Technology enabling voice calls over the internet.

Annex F: References

[1] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest; Fraud is the largest headline crime covered in the Crime Survey for England and Wales (CSEW)

[2] https://www.gov.scot/publications/scottish-crime-and-justice-survey-2023-24-main-findings/; Fraud is the biggest sub-type of crime covered in the SCJS

[3] The Northern Ireland Safe Community Survey does not separate out fraud, however given NI's lower crime volumes, fraud is the largest crime type in the UK

[4] https://www.gov.uk/government/publications/economic-and-social-cost-of-fraud-2023-to-2024

[5] As part of the Government's broader plans for Police Reforms, overall responsibility for Fraud, Economic Crime and Cyber Crime will transfer to the National Police Service with the NCA, and the NPS will be the lead agency for these crimes. Subject to the finding of the Independent Review of the Police Force Structures we will assess whether City of London Police's specialist services should transfer to the NPS or could be delegated and continue to be delivered by the City of London Police under NPS direction.

[6] https://assets.publishing.service.gov.uk/media/685ab0da72588f418862075c/E03360428_National_Security_Strategy_Accessible.pdf

[7] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest

[8] https://www.gov.uk/government/publications/economic-and-social-cost-of-fraud-2023-to-2024

[9] https://www.gov.scot/publications/scottish-crime-and-justice-survey-2023-24-main-findings/

[10] https://www.gov.uk/government/publications/economic-crime-survey-2024/economic-crime-survey-2024

[11] A recent review of fraud and computer misuse statistics for England and Wales (Review of fraud and computer misuse statistics for England and Wales) highlighted challenges with the coherence of fraud data sources, with CSEW highlighted as the most reliable data source on fraud.

[12] CSEW used a different methodology during the COVID-19 pandemic so direct comparison is not possible.

[13] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureoffraudandcomputermisuseinenglandandwalesappendixtables (Table 7)

[14] https://www.crestadvisory.com/post/understanding-and-addressing-fraud-against-children-and-young-people-an-action-plan (Full report)

[15] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureoffraudandcomputermisuseinenglandandwalesappendixtables (Table 8)

[16] https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-cyber-crime/experiences-of-victims-of-fraud-and-cyber-crime

[17] https://journals.sagepub.com/doi/10.1177/02697580261417364

[18] https://www.gov.uk/government/publications/economic-crime-survey-2024/economic-crime-survey-2024

[19] ibid

[20] https://www.gov.uk/government/publications/economic-and-social-cost-of-fraud-2023-to-2024

[21] https://academic.oup.com/ej/article-abstract/104/422/1/5158606

[22] [Publication Forthcoming] 2025 NAC Assessment

[23] Ibid

[24] https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf

[25] [Publication Forthcoming] 2025 NAC Assessment

[26] https://committees.parliament.uk/writtenevidence/125617/pdf/

[27] [Publication Forthcoming] 2025 NAC Assessment

[28] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/natureofcrimefraudandcomputermisuse

[29] https://www.ncsc.gov.uk/pdfs/guidance/data-breaches.pdf

[30] https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025

[31] [Publication Forthcoming] 2025 NAC Assessment

[32] ibid

[33] ibid

[34] ibid

[35] https://www.psr.org.uk/information-for-consumers/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age/

[36] [Publication Forthcoming] 2025 NAC Assessment

[37] ibid

[38] NFIB (February 2022) International Fraud Offending Recorded on Action Fraud: Professional estimation of international fraud offending

[39] https://link.springer.com/article/10.1007/s10611-024-10186-2

[40] https://www.taylorfrancis.com/chapters/edit/10.4324/9781315084572-19/organized-fraud-organizing-frauds-unpacking-research-networks-organization-michael-levi

[41] https://www.smf.co.uk/publications/international-fraud-comparison/

[42] https://www.nationalcrimeagency.gov.uk/images/campaign/NSA/2024/NSA%202025%20Website%20-%20PDF%20Version%20v1.0.pdf

[43] https://www.aseanact.org/resources/compound-crime-cyber-scam/

[44] https://www.bbc.co.uk/news/articles/cz6x1ql1yelo

[45] As part of the Government's broader plans for Police Reforms, overall responsibility for Fraud, Economic Crime and Cyber Crime will transfer to the National Police Service with the NCA, and the NPS will be the lead agency for these crimes. Subject to the finding of the Independent Review of the Police Force Structures we will assess whether City of London Police's specialist services should transfer to the NPS or could be delegated and continue to be delivered by the City of London Police under NPS direction.

[46] https://www.legislation.gov.uk/ukpga/2025/18/contents

[47] Ibid

[48] https://www.unodc.org/documents/treaties/COP12/Resolutions/E/Resolution_12_2.pdf

[49] https://www.mobileuk.org/news/uk-mobile-industry-blocks-one-billion-scam-messages

[50] https://www.met.police.uk/elaborate

[51] https://assets.publishing.service.gov.uk/media/690872f5c0dc8f1248417510/UK+Telecomunications+Fraud+Sector+Charter+Proof+v2.0.pdf

[52] https://assets.publishing.service.gov.uk/media/65688713cc1ec5000d8eef96/Online_Fraud_Charter_2023.pdf

[53] https://www.legislation.gov.uk/ukpga/2023/50

[54] ibid

[55] https://www.psr.org.uk/information-for-consumers/unmasking-how-fraudsters-target-uk-consumers-in-the-digital-age (page 28)

[56] https://www.psr.org.uk/media/2oflsqit/psr_app-victim-fraud-2025_report_web_version.pdf (page 10)

[57] https://www.legislation.gov.uk/ukpga/2024/13/contents

[58]https://assets.publishing.service.gov.uk/media/6170144f8fa8f529777ffc6f/Retail_Banking_Sector_Charter.pdf

[59]https://www.psr.org.uk/information-for-consumers/app-scams-reimbursement-dashboard/

[60]https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2025

[61]https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2025

[62]https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest

[63]https://fidoalliance.org/wp-content/uploads/2025/10/FIDO-Passkey-Index-October-2025.pdf

[64]https://www.nationalcrimeagency.gov.uk/news/nca-launch-first-ever-campaign-to-protect-men-against-crypto-investment-fraud

[65]https://www.gov.uk/government/publications/regulatory-regime-for-cryptoassets-regulated-activities-draft-si-and-policy-note

[66]https://www.legislation.gov.uk/ukpga/2023/56/contents

[67]https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-act-outline-transition-plan-for-companies-house/economic-crime-and-corporate-transparency-act-outline-transition-plan-for-companies-house

[68]https://www.gov.uk/government/publications/striking-off-or-dissolving-a-limited-company/striking-off-or-dissolving-a-limited-company (section 2.2)

[69]https://www.gov.uk/government/news/insolvency-service-welcomes-budget-funding-to-help-tackle-rogue-directors

[70] National Fraud Investigation Bureau (2025) ‘Fraud and Cyber-Crime, Annual Assessment 2024-2025’

[71]https://cfit.org.uk/digital-verification-coalition/

[72]https://www.legislation.gov.uk/ukpga/2023/56

[73]https://www.cps.gov.uk/cps/news/organisations-must-prepare-now-new-fraud-prevention-law

[74]https://www.copfs.gov.uk/about-copfs/news/new-guidance-expands-self-reporting-for-economic-crimes/

[75]https://www.gov.uk/government/publications/offence-of-failure-to-prevent-fraud-introduced-by-eccta/economic-crime-and-corporate-transparency-act-2023-guidance-to-organisations-on-the-offence-of-failure-to-prevent-fraud-accessible-version

[76] https://stopthinkfraud.campaign.gov.uk/?useContentAccordionItems=myy81&lang=en-US

[77] https://parentzone.org.uk/article/problem-hiding-plain-sight

[78] https://cybertoolkit.service.ncsc.gov.uk/?utm_source=NCSCResultsBlog&utm_medium=ResultsBlog&utm_campaign=PublicBeta&_gl=1*1gt5awd*_ga*MTI0NDAxNzI4NS4xNzYzNDg0MzMy*_ga_FMH2FBTCEP*czE3NjM0ODQzMzEkbzEkZzEkdDE3NjM0ODQzMzckajU0JGwwJGg3NDE2ODY1MjA

[79] https://nationalcrcgroup.co.uk/

[80] https://www.gov.uk/government/news/regulator-refreshes-guidance-as-it-reveals-600-cases-related-to-fraud-in-the-last-year

[81] https://www.ncsc.gov.uk/cyberessentials/overview

[82] https://www.betterhiringinstitute.co.uk/resources-hub/tackling-hiring-fraud-2-0

[83] Subject to the finding of the Independent Review of the Police Force Structures we will assess whether City of London Police’s specialist services should transfer to the NPS or could be delegated and continue to be delivered by the City of London Police under NPS direction.

[84] https://www.ukfinance.org.uk/news-and-insight/blog/vulnerable-victims-notifications-bringing-together-banks-and-law-enforcement

[85] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/756-nca-system-prioritisation-priorities-2025/file; https://www.rusi.org/explore-our-research/publications/emerging-insights/following-fraud-role-money-mules

[86] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/756-nca-system-prioritisation-priorities-2025/file

[87] https://www.legislation.gov.uk/ukpga/2023/29/contents

[88] https://www.tradingstandards.uk/media/documents/news--policy/impact-of-trading-standards-video-and-content/impact-of-trading-standards-in-statistics.pdf

[89] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/latest

[90] https://www.gov.uk/government/statistics/criminal-justice-system-statistics-quarterly-june-2025 (Outcomes by Offence Tool, including offences: 51, 52, 53.4, 53.6, 53B.1, 53C, 53D, 53E, 53F, year ending September 2025)

[91] https://www.gov.uk/government/news/swift-and-fair-plan-to-get-justice-for-victims

[92] https://www.gov.uk/government/collections/criminal-court-statistics

[93] https://www.gov.uk/government/collections/crime-outcomes-in-england-and-wales-statistics

[94] https://questions-statements.parliament.uk/written-statements/detail/2026-01-26/hcws1272

[95] https://assets.publishing.service.gov.uk/media/67e279b64fed20c7f559f558/Disclosure_in_the_Digital_Age_-_Independent_Review_Report_CP1285_WEB_0.1.pdf

[96] committees.parliament.uk/publications/50269/documents/271665/default/

[97] https://www.gov.uk/government/publications/public-authorities-fraud-error-and-recovery-bill-2025-factsheets/psfa-civil-penalties-powers-in-the-public-authorities-fraud-error-and-recovery-bill-factsheet

[98] https://assets.publishing.service.gov.uk/media/64539087faf4aa0012e132cb/Fraud_Strategy_2023.pdf

[99] https://www.gov.uk/government/publications/economic-crime-plan-2-outcomes-progress-report/economic-crime-plan-2-outcomes-progress-report#approach-to-the-ecp2-outcomes-framework-and-data-development

[100] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables (A1)

[101] https://www.gov.uk/government/publications/economic-crime-survey-2024/economic-crime-survey-2024

[102] Data development: Further work to measure fraud against businesses would be required to track change.

[103] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables (A1)

[104] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables (A4)

[105] https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2025 (Calculated by dividing number of cases by gross loss for both APP and unauthorised frauds.)

[106] https://colp.maps.arcgis.com/apps/dashboards/0334150e430449cf8ac917e347897d46

[107] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables (C1)

[108] https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/half-year-fraud-report-2025

[109] High harm includes: Cheque, plastic card and online bank accounts (not PSP), Mandate fraud, Dating scam, Financial investments & Fraud by abuse of position

[110] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables (C3), High Harm fitted NFIB codes: Fraud by abuse of position NFIB19 Share/bond sales or boiler room fraud NFIB2A4 Pyramid or Ponzi

schemes NFIB2B Prime bank guarantees NFIB2C Time shares and holiday club fraud NFIB2D Other financial investment NFIB2E Dating scam NFIB1D Cheque, plastic card and online bank accounts (not PSP) NFIB5A Mandate fraud NFIB5D

[111] https://www.gov.uk/government/publications/economic-crime-plan-2-outcomes-progress-report/economic-crime-plan-2-outcomes-progress-report#key-ecp2-indicators-and-data-development-updates

E03551200

978-1-5286-6251-2