Fraud Strategy 2026 to 2029: Disrupting crime, supporting economic resilience and delivering justice

Executive summary

About the Fraud Strategy

The Fraud Strategy 2026–2029 sets out the UK Government's plan to tackle fraud against individuals and businesses, combining disruption of criminal enablers, protection of potential victims and a stronger system-wide response. It is structured around three pillars:

- **Disrupt:** disrupting the tools, methods, systems and vulnerabilities exploited by criminals, making it harder for them to commit all forms of fraud. 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.
- **Safeguard**: safeguarding individuals and business by building an informed society, providing targeted support to those most vulnerable, and addressing the risk of financial exploitation. This involves strengthening public and business resilience through proactive policing, clear guidance and an expanded 'Stop! Think Fraud' campaign.
- **Respond**: improving reporting, victim support, investigation and justice outcomes

The Strategy applies across the public sector, law enforcement and intelligence community, and key industries including **telecommunications**, **online and technology platforms**, **cyber / national security**, as well as financial services, regulators, businesses and charities.

The Government will invest over £250 million between 2026 and 2029 to deliver the Strategy and delivery and compliance will be overseen through a strengthened governance model:

- The Home Secretary has overall responsibility, supported day-to-day by a Home Office Minister of State for fraud.
- The Economic Crime Strategic Board (ECSB) oversees the government's response to economic crime, with the Joint Fraud Taskforce (JFT) and a new Fraud Ministerial Accountability Group sitting beneath it.
- The JFT will continue to meet quarterly, bringing together ministers, law enforcement, regulators and industry as the top-level public-private forum on fraud.

- The **new Fraud Ministerial Accountability Group**, chaired by the Home Office fraud minister, will provide a cross-public sector forum for high-level strategic decisions and accountability.
- Progress on delivery will be reported annually to ministers to ensure ongoing scrutiny and strategic direction.

The Strategy sits within wider policing and security reforms, complementing the Police Reform White Paper, the transfer of overall responsibility for fraud, economic crime and cyber crime to the National Police Service with the NCA, and operational initiatives such as the National Fraud Squad, the new Report Fraud service, and closer alignment between fraud and cyber crime policing.

Key measures for ISPA:

I. Pillar 1: Disrupt

The Strategy sets out that the Government will collaborate with the telecommunications sector to deliver interventions that address the gaps and vulnerabilities that have enabled criminals to deliver fraudulent texts and calls to victims at scale.

- **To disrupt fraud, criminals must be denied access to the telecommunications network.**
- The Government recognises progress by the telecommunications sector, including the second **Telecommunications Fraud Charter,** expanding commitments to intelligence sharing, traceback schemes, network upgrades, AI tools, and improved victim support - **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.

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**.

- The call for evidence will gather views on interventions 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.

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 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.

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. The OCC is designed to accelerate the UK's response to online crime, initially **focused on fraud and high-volume cyber crime**. The OCC's key functions include:

- Collecting, combining, and rapidly analysing large volumes of data across its public and private sector partners to inform proactive action to address the online fraud and cyber crime threats, and support private sector partners to improve internal controls and resilience.
- Sharing information relating to **criminal abuse of websites, emails, and phone numbers** and criminals' behavioural data, to identify and disrupt illicit activities by **blocking calls, freezing accounts, taking down websites, and restricting social media accounts** with the digital and technology sectors.
- 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.

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.

Ofcom has committed to **robust monitoring and evaluation of the impact of the Online Safety Act**, focused on two core questions: what changes are services making to comply with their duties under the Act and are these changes translating into a safer life online for UK users.

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.

The Government will also:

- 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**.
- 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.
- Launch the public-private **Online Crime Centre** to share data and collaborate on interventions that eliminate online fraud at scale, to begin operations in **April 2026.**
- Sponsor the next Global Fraud Summit in Vienna in March 2026 with UNODC and INTERPOL and pursue international agreements and partnerships.

II. Pillar 2: Safeguard

From April 2026, the **Stop! Think Fraud campaign will expand** to cover a broader range of fraud types including high-harm frauds. Its broader ambition is to continue to work with industry, including technology and telecommunications companies, to encourage the uptake of protective behaviours by integrating messaging into their customer communications and delivering joint activity.

From 2026, the Home Office will also work to **raise awareness of existing tools** that the public can use to help detect and protect against fraud to help individuals identity and make use of available services, some of which are **embedded within telecommunications platforms**.

III. Pillar 3: Respond

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.

Other key interventions include operating the **new service Report Fraud from 2026**, which ensures streamlined reporting service, to provide a robust and improved reporting mechanism for victims of fraud. The Government will also introduce a **Fraud Victims Charter in 2027** which will set out a minimum standard of care across all support providers, to ensure consistent victim support. Finally, 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. As part of this, the Home Office will support INTERPOL to establish a **Global Fraud Taskforce by 2029**.

The Fraud Threat in detail: key figures form the strategy

Fraud against individuals and businesses is now the largest crime type in the UK, costing the economy **£14.4 billion in 2023–2024**. It is widespread: in the year ending September 2025 there were over 4 million estimated offences, accounting for **45% of all crime** in the Crime Survey of England and Wales; and **one in four UK businesses** with more than one employee experienced fraud in the previous twelve months – around 389,000 businesses and an estimated 6.04 million instances of fraud.

The highest proportion of fraud victims are currently aged 45–54 and 55–64, but risk is rising disproportionately among young people. In the year ending March 2024, 74% of frauds involved a financial loss; in 3% of cases the loss was £10,000 or more, equating to around 75,000 high-loss incidents.

Fraud is increasingly technology-enabled. Almost **half of all estimated frauds are online-enabled**, and criminals continually adapt to new security measures. When two-factor authentication became standard, they shifted to social engineering and SIM-swapping to obtain one-time passcodes and hijack mobile phones. The introduction of spam filters prompted another change in tactics, with SMS messages restructured and alternative text formats used to bypass firewalls. In 2023, **53% of reported Authorised Push Payment (APP) fraud cases involved social media, messaging and call platforms**, 13% involved auction, purchase and listing platforms, and 12% involved telecommunications platforms.

Fraud is also a global, industrial-scale threat. Over two-thirds of cases have an international element, and overseas networks are highly organised and technologically advanced. **Criminals use VPNs and Voice over Internet Protocol to mask their locations and spoof UK numbers**, and many networks operate from organised call centres or secure scam compounds dedicated to large-scale fraud operations.