Home Office

UK Telecommunications Fraud Sector Charter

5 November 2025

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at homelandsecurityfraudpolicyunit@homeoffice.gov.uk

Contents

Ministerial Foreword

Fraud is estimated to be the UK's most prevalent crime type according to the Crime Survey for England and Wales, and its impact is felt across every corner of society, from vulnerable individuals to major businesses and public services. The telecommunications sector sits at the heart of our digital infrastructure, and with that comes both opportunity and responsibility. Criminals exploit connectivity to deceive and defraud, but through collaboration, innovation, and determination, we can make it harder for fraudsters to abuse the network and reach consumers. This means protecting the public, and their money, from scammers. Fraud is also a drag on growth.

This Charter represents a landmark commitment from the telecoms industry to tackle fraud head-on. It builds on the progress made since 2021 on preventing scam calls and texts and protecting its customers, and sets out a bold, practical roadmap for action, preventing scam calls and texts, strengthening data sharing, harnessing AI to prevent scams, and supporting victims with compassion. Tacking fraud is also a major contributor to the government's growth mission.

Government stands firmly alongside the sector in this fight. We will continue to convene, support, and challenge all partners to go further and faster, holding them to account for the commitments they make in this Charter. Together, we can make the UK a hostile environment for fraudsters and a safer place for everyone.

Rt Hon Lord Hanson of Flint

Minister of State (Lords Minister)
Home Office

Industry Foreword

Fraud is now the most common crime in the United Kingdom.

Every hour of every day, criminals seek to exploit the networks we run and the connectivity we provide to commit fraud against individuals, businesses, and public services. As an industry we invest significant sums of money every year in protecting our customers and UK plc from these criminal attacks.

But this is not a fight we can win alone. This Charter marks the next step in our sector's fight against fraud. Tackling fraud must be a shared endeavour, and eroding criminals' ability to undertake it relies not just on our sector, but on the combined efforts of our partners across the ecosystem.

Our technology underpins and enables our banking systems, the social media platforms we access on our mobile devices, and the government services we rely on. Our economy and society depend on these fundamental technologies. And so, we must work together to tackle this common threat.

We have made great progress since signing the first Telecoms Fraud Sector Charter in 2021. But as fraud evolves, so must our efforts. We wish to make the UK a harder target for fraudsters, and a safer place for the public.

This Charter sets out practical, measurable actions that will deliver real change - from expanding trusted data sharing and enhancing call security, to using artificial intelligence responsibly, and supporting victims with compassion and speed.

This Charter builds on the strong foundations we already have, and goes much further:

- To prevent and detect fraud at source - identifying and disrupting criminal activity before it reaches customers.
- To protect consumers and businesses, ensuring interactions on our networks are trusted and secure.
- To improve public awareness, build on our work with law enforcement, and enhance the protection and support we give to victims of fraud.
- To be nimble and work collaboratively across sectors, sharing data, insight, and innovation to outpace the threat.

Together, these commitments form more than a plan - they form a promise: that the telecoms industry will play its full part in tackling the fraud epidemic that the UK faces.

Brian Webb

Chief Security Officer, BT EE

Chair, Communications Crime Strategy Group

Section 1: Mobile Networks

Signatories: Communications Crime Strategy Group

Collaborative Data Sharing to Tackle Fraud

Mobile networks will strengthen and expand trusted, responsible data and intelligence sharing to prevent fraud and protect consumers.

Signatories will:

- Expand the types and volume of data shared across the sector, through platforms such as Cifas, Stop Scams UK, and with law enforcement and the tech and banking sectors, to better identify, isolate, and prevent fraud.
- Underpinned by effective data sharing, commit to work in partnership with law enforcement and industry partners to tackle criminal enablers, disrupting fraud at scale.
- Maintain and promote the 12 existing banking-sector fraud prevention APIs (Application Programming Interface).
- Establish and participate in cross-sector workshops (convened with Home Office support) within 6 months to design scalable, collaborative data-sharing models between telecoms, banking, and tech, including agreed use cases, safeguards, and implementation plans.
- Prevent customers from inadvertently accessing known scam sites and fraudulent domains by working with the NCSC on their Share and Defend programme to increase its protective coverage.

Our goal is to create a seamless, multi-sector data-sharing ecosystem that enables faster detection of bad actors, reduces fraud across industries, and ensures appropriate safeguards for consumers.

Timeline

- **Within 6 months:**
  - Working groups established.
  - First cross-sector workshops held.
- **Within 12 months:**
  - Agreed cross-sector data-sharing models finalised.
  - Expanded data sharing in place with measurable uptake and impact across sectors.
  - Increased usage of existing fraud prevention APIs.

Strengthening Trust in Voice Communications

The telecoms industry will reduce fraud and abuse in voice communications, particularly the spoofing of UK numbers, by improving the security, traceability, and reliability of call infrastructure.

Signatories will:

- Work with Ofcom to develop a call tracing process that can help address the challenge of scam and fraudulent calls being received by UK subscribers.
- Support the adoption of modern network features, such as VoLTE (Voice over Long-Term-Evolution) to improve visibility, control, and fraud prevention.
- Establish partnership opportunities and forums to identify shared challenges, align on good practice, and deliver scalable solutions that strengthen trust in the voice channel.
- Engage with partners in banking and tech to improve cross-industry coordination and intelligence sharing with Home Office support.

Timeline

- **Within 6 months:**
  - Agree key focus areas and priority solutions for the sector.
  - Establish working group to oversee traceback implementation and network feature upgrades.
- **Within 12 months:**
  - Launch operational traceback across participating networks.
  - Deliver measurable adoption of modern network features such as VoLTE.

Securing Network-Originated SMS as a Trusted Channel

Mobile networks will preserve network-originated SMS as a trusted and secure channel for communication, protecting its continued use by businesses, public services, and consumers. Where networks do not have control over messaging services (such as RCS messaging), we will work with others to enhance fraud prevention measures, bringing them in line with existing work on SMS.

Signatories will:

- Strengthen sender verification processes to prevent spoofing and unauthorised use of trusted sender IDs.
- Enhance vetting and onboarding procedures for commercial SMS customers to ensure only legitimate users can send messages via telecoms networks.
- Share intelligence on emerging threats across the sector and with other industries, such as financial services and technology platforms, to deliver a coordinated response.
- Propose that RCS providers fall in line with CCSG members' existing fraud prevention work on SMS, including intelligence and 7726 data sharing. This proposal will be formally tabled in the Home Office convened tech, telco and banking roundtables discussed in the first section of this Charter.
- Develop and adopt common standards to reduce fraud and abuse across all network-originated messaging channels.
- Engage with Ofcom's consultation on proposals to tackle mobile messaging scams.

Timeline

- **Within 6 months:**
  - Identify key risks, gaps, and opportunities for alignment.
  - Establish working groups on SMS security.
- **Within 12 months:**
  - Deliver strengthened sender verification and onboarding processes across participating networks.
  - Launch updated sector-wide standards for secure messaging.

Using AI Responsibly to Prevent Fraud

Mobile networks will continue to harness artificial intelligence to detect, disrupt, and prevent fraud, while safeguarding privacy, transparency, and consumer trust.

Signatories will:

- Establish a dedicated AI Fraud Prevention Working Group to coordinate activity across the sector.
- Map current AI tools in use across networks and assess their effectiveness in fraud detection and prevention.
- Develop and adopt common principles for the ethical deployment of AI in fraud prevention, aligned with legal and regulatory requirements.
- Share real-time threat intelligence and case studies where AI has successfully disrupted fraud.
- Work with cross-sector partners to identify new AI-enabled threats and design mitigation strategies.

Timeline

- **Within 12 months:**
  - AI Fraud Prevention Working Group established and operational.
  - Sector-wide mapping of AI tools and use cases completed.
  - Ethical principles agreed and published.
  - Intelligence-sharing framework for AI-related threats operational.

Raising Customer Awareness – Stop! Think Fraud Campaign

Mobile networks will help consumers recognise fraudulent activity, take protective action, and report scams by aligning with and promoting the Government's **Stop! Think Fraud** campaign.

Signatories will:

- Incorporate Stop! Think Fraud messaging and branding across customer communications to ensure consistent, high-impact fraud prevention messages.
- Develop and share industry-specific content that supports the national campaign narrative while addressing telecoms-related fraud threats.
- Coordinate with the Stop! Think Fraud campaign team and the Home Office to plan and align activity, ensuring maximum reach and effectiveness.
- Support cross-sector collaboration to ensure a single, clear public message on fraud prevention.

Timeline

- **Immediately:**
  - Networks review and adopt Stop! Think Fraud campaign messaging from signing the Charter.
- **Within 6 months:**
  - Long-term coordinated plan with Stop! Think Fraud agreed and in delivery.

Improving Staff Awareness

Frontline staff play a critical role in preventing fraud, detecting suspicious activity, and supporting vulnerable customers. Mobile networks will strengthen internal defences by agreeing and adopting common best practice to prevent fraud, particularly account takeover, and ensuring all staff are trained to meet these standards.

Signatories will:

- Agree and document sector-wide best practice to prevent fraud, including measures such as requiring two-factor authentication before account transfers.
- Train all relevant staff to follow these standards, with a focus on identifying and stopping fraud before it occurs.
- Continue to deliver training on recognising fraud risks, supporting victims, and responding effectively when incidents occur.
- Work with the National Trading Standards' Friends Against Scams team (or an equivalent) to share large-operator training methods and resources with smaller operators, ensuring consistent capability across the sector.
- Maintain continuous quality assessment of training effectiveness and update content to reflect emerging threats.

Timeline

- **Within 12 months:**
  - Sector-wide best practice for fraud prevention agreed and published.
  - Staff training programmes updated to meet agreed standards and rolled out across all participating operators.
  - Friends Against Scams (or equivalent) collaboration established and delivering training support to smaller operators.

Supporting Victims of Fraud

Mobile networks will provide consistent, compassionate, and effective support to individuals who have fallen victim to fraud, helping them recover and regain confidence.

Signatories will:

- Develop and adopt a set of shared sector-wide principles for victim support.
- Create clear, practical guidance for victims, including steps to secure accounts and protect against further harm.
- Improve signposting to specialist fraud support services and law enforcement reporting channels.
- Ensure frontline staff follow a consistent approach to victim engagement, informed by victim feedback and best practice.
- Use regular victim surveys to monitor the effectiveness of victim support and drive continuous improvement.
- Commit to the majority of cases being resolved within 21 days one year on from this Charter being signed, and a target of 14 days two years after Charter signing.

Timeline

- **Within 6 months:**
  - Shared victim support principles developed and agreed.
- **Within 12 months:**
  - 21-day fraud case resolution for the majority of cases.
- **Within 24 months:**
  - 14-day fraud case resolution for the majority of cases.
  - Principles fully adopted and implemented across all participating operators.

Collaboration with Law Enforcement and Government

Fraudsters operate on a huge scale, targeting thousands of people and stealing millions of pounds. By focusing on the criminals causing the most harm, mobile networks can help stop scams before they reach the public.

Signatories will:

- Establish a SIMs/eSIMs working group to understand the scale of the threat of bogus pay-as-you-go identities used to commit fraud.
- Public Private Operations Board participation - Share targeted intelligence with law enforcement through the Fraud Targeting Cell. This will include providing a small number of high-quality UK-based intelligence packages that meet national or regional policing priorities. The aim is to help law enforcement use their resources to go after the “directing minds”, key enablers, and ultimate beneficiaries of fraud abusing the telecoms network.
- Establish an industry / law enforcement working group to understand how SIM Farms and SMS blasters are being utilised, share intelligence and provide evidence to drive the closure of illegal activity

Timeline

- **Immediately:**
  - Begin sharing intelligence on major fraudsters with law enforcement through the Fraud Targeting Cell.
- **Within 6 months:**
  - Agree and implement a shared process for identifying and prioritising the most harmful offenders. Establish SIM Farm/Blaster working group.

Section 2: Business-to-Business Voice and Telephony

Signatories: Comms Council UK

Collaborative Data Sharing to Tackle Fraud

CCUK Council and the Fraud and Scams Group, as members of the voice and telephony sector, will improve and expand cross-sector collaboration on intelligence sharing and technological solutions to combat fraud and protect businesses.

Signatories will:

- Work with the Network Interoperability Consultative Committee (NICC) to create a proof-of-concept API that enables trusted sharing of fraud intelligence (such as suspicious numbers, sender IDs, or activity patterns).
- Broaden industry participation in the National Trading Standards data-sharing scheme, established by CCUK and the NTS in January 2025, to strengthen collective defences against fraud.
- Commit to work in partnership with law enforcement and industry partners to tackle criminal enablers, disrupting fraud at scale, underpinned by effective data sharing
- Maximise the impact of data sharing by partnering with established industry and cross-sector initiatives and enabling reciprocal arrangements where appropriate.
- Explore and evaluate technological advancements that can help in the fight against fraud.

Timeline

- **Within 6 months:**
  - Promote NTS data-sharing scheme.
  - Begin engagement with NICC on API-driven data sharing proof-of-concept.
- **Within 12 months:**
  - Report progress on API proof-of-concept and contribution to data sharing to tackle criminal enablers.
  - Report on NTS alerts, engagement and project progress.
  - Provide updates on technological advancements and their impacts.

Traceback - Engaging with Key Groups to Develop Effective Technical Solutions to Fraud

Work with industry partners to develop and promote effective technical solutions to detect and stop fraudulent activity. By sharing knowledge and aligning on robust technical standards, we will strengthen defences across the sector and ensure a rapid response to emerging threats.

Signatories will:

- Commit to actively engage with the development of a UK Traceback solution, allowing providers to trace the origin of suspicious or fraudulent calls across interconnected networks. By doing so, operators will be able to more quickly identify the source network, and, where possible, the origin of scam calls, helping to disrupt fraud at its origin.

Timeline

- **Within 6 months:**
  - Continue engagement on a UK Traceback solution.
- **Within 12 months:**
  - Share evaluation findings and recommendations for sector-wide adoption

Adapt and Promote Best Practice Guidance

Implement and continuously improve best practices for our members to prevent the misuse of voice and telephony services for fraud. This will centre around continuing to promote and regularly update CCUK's best practice guidance to our membership to raise standards and reduce opportunities for fraudulent behaviour using voice and telephony.

Signatories will:

- Continue to implement existing CCUK guidance on preventing misuse of sub-allocated and assigned numbers and monitoring for fraudulent calling patterns.
- Review and update guidance in response to new threats regularly.
- Encourage wider adoption of the guidance by actively engaging all CCUK members and issuing regular reminders.
- Record all guidance produced and set review dates to ensure it remains current.

Timeline

- **Within 6 months:**
  - Maintain and update best practice guidance.
  - Promote best practice guidance through internal communications with members.
  - Regularly review best practice guidance as and when new threats arise.
- **Within 12 months:**
  - Submit summary to the Home Office of new and updated guidance.
  - Conduct annual survey for members to self-declare compliance with best practice in key fraud areas.
  - Provide case studies showing where guidance has been implemented and its impact.

Improve Staff and Customer Awareness of Fraud

Frontline staff play a critical role in preventing fraud, detecting suspicious activity, and supporting customers. The voice and telephony sector will raise awareness of fraud among CCUK member employees and customers to staff and customers to improve detection, prevention, and reporting.

Signatories will:

- Create best practice guidance for members to include fraud messaging in customer communications, websites, and contracts.
- Promote the government led ‘Stop Think Fraud’ campaign.
- Conduct proactive press outreach to business, technology and national press to raise awareness of the challenge fraud poses to British businesses and how to prevent it.
- Deliver a year-round programme of learning events for members, focused on fraud.
- Promote relevant external training opportunities.

Timeline

- **Within 6 months:**
  - Add fraud guidance page to CCUK website.
  - Promote the government led Stop! Think Fraud campaign.
  - Continue press outreach to business, technology and national press.
- **Within 12 months:**
  - Report on webinars/training delivered, with attendee numbers.
  - Provide case studies from members on the impact of training and guidance.
  - Showcase examples of fraud messaging implementation (e.g. website snapshots).

Support Business Victims of Fraud

Commit to delivering clear, consistent, and practical guidance for our members to support business customers who fall victims to fraud. By adopting shared principles and guidance, we will support businesses in recovering from fraudulent activity, strengthen their defences, and reduce the likelihood of fraud on voice and telephony networks.

Signatories will:

- The CCUK Fraud and Scams Group and Council will jointly develop a set of shared principles for business victim support.
- Produce clear, practical guidance for members to help business customers by improving signposting.
- Promote adoption of these principles across the voice and telephony sector, ensuring consistent support for affected businesses.

Timeline

- **Within 6 months:**
  - Develop business victim support principles.
- **Within 12 months:**
  - Finish development and promote principles across the industry and collect confirmations of intentions of signing up.
- **Within 18 months:**
  - Full adoption of principles by Council and Fraud & Scams Working Group.

Glossary

Term	Definition
CCSG	The Communications Crime Strategy Group - a collaborative body focussed on tackling telecoms-related crime and security issues, including taking the industry lead on fraud.
CCUK	Comms Council UK – represents business-to-business telecoms providers.
API	Application Programming Interface – a set of tools and protocols for building software and enabling data sharing.
VoLTE	Voice over Long-Term Evolution – a standard for high-quality voice calls over LTE networks.
RCS	Rich Communication Services – an advanced messaging protocol intended to replace SMS.
7726	A short code used to report spam or fraudulent messages to mobile operators.
SIM Farm	A setup using multiple SIM cards to send bulk messages, often used in fraudulent activity.
SMS Blaster	A tool used to send mass SMS messages, potentially for scams or spam.
NICC	Network Interoperability Consultative Committee – a UK body that develops interoperability standards.
NCSC	National Cyber Security Centre – UK government agency providing cyber security guidance and support.
Stop! Think Fraud	A UK Government campaign aimed at raising public awareness of fraud.
Friends Against Scams	A National Trading Standards initiative to protect and support scam victims.
Fraud Targeting Cell	A collaborative unit for sharing intelligence with law enforcement to target high-impact fraudsters
SIM/eSIMs	Subscriber Identity Module / Embedded SIM – used to identify and authenticate users on mobile networks.


5G