CCUK Fraud Summit Briefing

15 April 2026

Contact

For more information, please contact:

Comms Council UK
team@commscouncil.uk
020 3397 3312
@commscounciluk

The second **CCUK Fraud Summit** brought together representatives from telecoms, as well as regulators, law enforcement bodies, and civil services, to share insights on how to tackle fraud effectively. The keynote speaker at the event was **Rt Hon Lord Hanson of Flint**, Minister of State at the Home Office.

Throughout the day, representatives from **Ofcom, National Crime Agency, Home Office, Vonage, Gamma, BT, VM02 and more** joined our sessions and panels. The focus of the Summit was cross-border fraud mitigation and supporting the sector's wider data-sharing ambitions and finding coordinated, effective responses to fraudulent calls. The day featured panels, expert presentations, and opportunities for networking.

The CCUK Fraud Summit highlighted that only a coordinated approach - combining international cooperation, system data-sharing and practical tools like traceback and number intelligence - between industry, regulators, and government can tackle telecoms-enabled fraud and better protect customers.

Lord Hanson Keynote Speech

Lord Hanson, the Fraud Minister, centred his keynote on the need to make the UK a hostile environment for fraudsters, and, in order to make this a reality, to coordinate a system-wide, cross-border response between government, the private sector, and law enforcement. He also provided a high-level overview of recent initiatives and future reforms the government is driving to tackle fraud.

The Minister framed fraud as both personal and economically corrosive, a crime that impacts lives and businesses, drags on growth and undermines confidence in online markets and the telecoms sector. He stressed that criminals are unregulated, agile, and increasingly using AI, and that the UK must respond with equal agility.

Lord Hanson set out how the Government's new **Fraud Strategy 2026–2029** provides a roadmap to make the UK a more hostile environment for fraudsters to operate. He underlined that mobile operators and VoIP providers hold powerful levers to tackle fraud at scale, and that the Government has clear expectations of how it will work together with industry under the Strategy. Positioning it as a core initiative within the Strategy, Lord Hanson highlighted the **Online Crime Centre** (OCC) as a step-change in the UK's ability to prevent fraud before it reaches the public. For the first time, the OCC will bring together the Home Office, NCA, City of London Police, the wider intelligence community and private-sector partners from telecoms, finance and technology to combine data, analyse trends and coordinate interventions.

The Minister pointed to the **Telecommunications Fraud Sector Charter** as a core tool, noting that, since its publication, it has strengthened data-sharing arrangements, driven progress on SMS verification, and work on traceback has started. He stressed that the Charter is "a commitment, not a promise" and government will be holding the sector to account.

Looking ahead, Lord Hanson described **telecoms traceback** as a potential turning point, giving investigators the ability to trace scam traffic back through interconnected networks and shut down criminal infrastructure. He acknowledged that AI is both a threat and a tool: while criminals are already exploiting it, government and industry are beginning to use it to detect and remove fraudulent websites and patterns of abuse. Throughout, he stressed that effective enforcement depends on the whole communications ecosystem working together. He also stressed the need to improve the experience for victims, pointing to **Report Fraud** and current work to develop a **Fraud Victims Charter**, setting out what victims should be able to expect from the system.

Finally, Lord Hanson underlined that most large-scale fraud has an **international dimension** and highlighted the UK's role in sponsoring the **Global Fraud Summit** in Vienna with UNODC and INTERPOL, which brought together over 100 countries. He also referenced bilateral **Memoranda of Understanding** with high-priority countries, including Nigeria.

Tracey's Year to Date Speech

In her Year to Date Speech, CCUK Chair Tracey reflected on the journey since the first Fraud Summit in March 2025 and set the stage for the discussion. Her speech focused on recent work and progress to tackle fraud, and the focus going forward, underscoring the need for collaboration and interconnection particularly given the evolution of criminal behaviour.

Consolidating progress since the first Fraud Summit: Tracey noted that last year's inaugural summit, bringing together over 150 figures from government and industry, proved there is both the appetite and capability to do more. She thanked sponsors and attendees, stressing that this shared sense of responsibility is vital to tackle fraud.

Navigating an evolving sector: Highlighting the evolving nature of the industry, particularly as it transits from the era of traditional telephone networks to a fully digital, IP-based environment. Tracey pointed out the need to ensure the clear benefits from this shift (innovation, flexibility, and richer services) are not overshadowed by the increasingly evolution of criminal behaviour. She stressed that, since criminals do not see boundaries, but rather an interconnected system to manipulate, sectors must be as interconnected as the networks they manage, which requires a shared understanding and trust between actors that a collective response is needed.

Turning commitment into action: Tracey pointed to the signing of the Telecommunications Fraud Sector Charter in November 2025 as a major milestone and an operational roadmap, with government regularly checking in and holding industry to account. As part of CCUK's work to meet the commitments, she outlined the new Fraud and Data-Sharing Workshops with the Home Office and industry. Alongside these flagship initiatives, Tracey pointed to ongoing efforts to refresh best-practice guidance for members of all sizes, promote the Stop! Think Fraud public awareness campaign, contribute to early traceback work, and develop Business Victim Principles to support providers managing incidents among their business users. She also highlighted the crucial role of the Fraud and Scams Working Group and the National Trading Standards information-sharing service as hubs for intelligence, best practice and experimentation.

Looking ahead to a seamless, multi-sector ecosystem: Looking forward, Tracey stressed the need to move from "joining the dots" to building a seamless, multi-sector data-sharing ecosystem, underpinned by a long-term architecture of cooperation. This includes strengthening international, cross-border collaboration, and supporting developments such as the forthcoming Online Crime Centre.

Tracey concluded by calling for ambition, practicality and unity from all stakeholders, urging them to channel the day's discussions into clear, collective actions.

Art of the Possible: International Joining the Dots panel

Panellists: Alex Jennings – CCUK Council, John Ayers – ITG, Justen Davis – Somos, Ian Hindle – NICC

This session provided an international perspective on how advanced traceback and telephone-number intelligence frameworks can transform fraud prevention. Panellists explored how better data, numbering repositories and neutral traceback models can "join the dots" turning high-level collaboration into concrete operational tools.

- **Building the technical infrastructure to operate at scale**: The session opened highlighting that with over 40,000 players in the telecoms ecosystem, informal data-sharing alone is not enough. Two building blocks are now needed in the UK: a modern traceback capability and a numbering repository, going beyond today's high-level databases so that providers can see, in near real

time, how numbers are allocated, used and potentially abused.

- **Traceback as an accountability tool**: John Ayers shared the experience of the Industry Traceback Group (ITG), originally created to tackle illegal telemarketing and nuisance calls in North America as a certified neutral party. The presentation highlighted that the TG now runs around 1,000 tracebacks per month through a secure portal, roughly 80% of cases are fully completed, and 65–70% of those completions lead to action by providers or enforcement through an end-to-end process. The case study showed that success depended on strong participation from carriers from the outset and a clear, trusted governance model, creating a structured pathway for providers and authorities to act on bad traffic, including in cooperation with partners in other countries.
- **Comprehensive DNO and number intelligence**: Justen Davis outlined how Somos has built a Comprehensive Do Not Originate (DNO) and telephone-number intelligence framework across the North American Numbering Plan – and what that might mean for the UK. The presentation demonstrated how a real-time DNO ecosystem, layered with behavioural and network intelligence, allows providers to block calls from numbers that should not be in use at all, significantly reducing robocalls and abusive traffic. For the UK, he noted a similar opportunity: with large proportions of invalid and unallocated numbers, there is clear scope to tighten control over numbering, identify who is enabling misuse, and give enterprises and providers tools to feed into a shared DNO and intelligence framework.
- **Standards to scale best practice in the UK**: Ian Hindle set out how NICC's technical standards work underpins many of the capabilities discussed on the panel. Recent work has focused on defining common technical approaches for caller identification, signalling and fraud-related controls, ensuring that any UK traceback and DNO solutions are interoperable across networks and consistent with international approaches; and providing a standards framework that allows Ofcom, industry and international partners to implement and evolve these tools coherently, rather than as isolated, proprietary solutions.

Oculeus presentation

Speaker: Eric Priezkalns

Eric Priezkalns used international case studies to show how different regulatory choices shape the scale of unwanted communications and scams, arguing that while the UK is performing better than other countries, it needs to tighten controls on numbering, caller identity and SMS sender IDs.

- **International case studies**: Eric Priezkalns shared examples to show how different countries are responding to scams and unwanted communications. He highlighted a Singapore case study as one of the best sources of data on scams migrating to India, noting that India now shows a strong pattern of improved control. He also referenced Nigeria's decision to instruct WhatsApp to ban certain activity, underlining that criminals do not care about silos or formal responsibilities – they simply move to wherever controls are weakest.
- **British experience**: The presentation contrasted British successes with the experience in other markets. In the UK, complaints are largely about unwanted communications, and levels of automated calls are lower than in countries such as the US or Australia. By comparison, Americans continue to complain heavily about unwanted calls, and in the US complaints about robocalls have never fallen below complaints about live calls.
- **Sender ID registries and operator responsibilities**: The session drew attention to the UK's voluntary SMS Sender ID registry, in contrast to countries where similar schemes are mandatory, and raised questions about how UK operators are using these tools to manage risk. One key lesson mentioned is that "the harder you look, the more you find" – deeper scrutiny consistently surfaces more problems, reinforcing the need to look closely across networks and borders if scams are to be effectively controlled.

NTS Update and Truecall session

Speakers: Richard Clarke - NTS, Adam Carter - NTS, Steve Smith - trueCall

This session showed how landline call-blocking data, when combined with National Trading Standards' disruption work and industry cooperation, can significantly reduce harm to older and vulnerable people – but only if organisations share data and improve transparency over who is on the network and who owns numbers.

- **Landline fraud**: Steve Smith explained that trueCall has been blocking nuisance and scam calls for around 20 years, sitting between the phone and the phone line and blocking over 95% of unwanted calls. He stressed that the landline remains critical for a key demographic: around 80% of over-70s have a landline, and more than half of the calls they receive are made by scammers. TrueCall devices are now used widely by local authorities, charities and police forces, and the data from thousands of opted-in units gives a detailed picture of all calls received – not just the small fraction that generate complaints. By combining this metadata with the caller descriptions on Who-Called.co.uk, trueCall has built tools to browse and cross-match both datasets, identify top scam numbers and categories, estimate call volumes, and identify range-holders. This intelligence is already used by agencies including the ICO, Ofcom, the National Fraud Intelligence Bureau, National Trading Standards and the NCA.
- **National Trading Standards - a two-way street:** Adam Carter set out who the National Trading Standards Scams Team are and how they work with telecoms. He emphasised that the relationship is a two-way street: NTS uses tools like trueCall to generate leads and alerts, but also needs providers to come to them with concerns about dubious clients or traffic. His core message was the need for a shared view of the threat built on data-sharing, not isolated datasets and one-off conversations.
- **From alerts to disruption:** Richard Clarke illustrated what this looks like in practice. Since 2019, more than 7,000 trueCall units have been deployed to consumers and agencies, blocking millions of scam and nuisance calls. Using this data and wider partnerships, NTS has blocked 6.5 million scam calls, removed 283 numbers, disengaged 14 criminal companies, identified and supported 5,288 victims and saved over £2 million for UK consumers. He described how NTS targets "professional enablers" and uses an alert system to notify multiple telecoms providers when a fraudulent company, director or organised crime group is identified, sharing examples of this in practice. However, with teams often working in silos, criminals exploit gaps.

The team concluded with a straightforward ask: share data, engage with NTS alerts, and support efforts to create a Communications Provider Registry and a central numbering database, alongside broader participation in data-sharing efforts, so fewer scams reach consumers in the first place.

Fraud at the Coal Face

Speakers: Paul Morris - Vonage (Host), Laura Moore - Magrathea, Matt Dore - Gamma, Perry Wilks - BT, Kerry Smith - Virgin Media O2, Christie Grinham - bOnline

This session looked at fraud from the frontline perspective, drawing on real cases and operational experience from across the telecoms ecosystem. Panellists explored how scams move through complex supply chains, the practical trade offs between commercial priorities and robust controls, and the kinds of shared tools and data that would enable a more proactive, system wide response.

- **Building a network of "canaries":** Panellists discussed the need to move from reacting to individual incidents toward building an early warning system for suspicious activity. They described "canary" signals across networks such as unusual traffic patterns, rapidly changing CLIs and unexpected spikes that, if spotted and shared quickly, can help providers "run" before fraud becomes widespread.
- **Balancing friction and ease of use for small businesses:** Christie Grinham outlined how bOnline serves small businesses that need low cost, easy to adopt services, and how fraud controls can unintentionally slow innovation. To manage this, bOnline has developed fraud scoring and monitoring using IP geolocation and call spike analysis. When potential fraud is detected, services are blocked immediately and then subjected to risk based KYC checks, with panellists agreeing that smarter, shared approaches to onboarding and known bad actors would benefit the whole chain.
- **Managing risk through partner relationships:** Matt Dore described Gamma's position as one step

removed from end users and the need to "parent" a large base of partners. While the majority pose no problems, a small minority can generate disproportionate risk. The discussion emphasised proactive engagement, better communication and clearer expectations as key tools for managing relationships, especially where limited visibility of end use cases makes risk assessment harder.

- **Using data sharing to raise the cost of fraud:** Laura Moore highlighted Magrathea's experience in working with the National Trading Standards data sharing programme. She noted that industrial scale fraudsters are often sophisticated enough to pass standard KYC checks, and that effective disruption depends on making it harder and more expensive for them to operate across multiple providers. Offboarding bad actors and sharing intelligence through CCUK and other mechanisms was seen as essential to increasing their operating costs.
- **Traceback, registries and shared infrastructure:** Several panellists stressed that carriers which do not engage with traceback or respond to enquiries in a timely way pose heightened risk. Suggested priorities included a CP registry to provide proof of authenticity for communications providers and a common numbering database so that control of numbers is clearly understood. The panel concluded that the sector must avoid simply passing bad traffic along the chain, instead using tools such as traceback, DNO lists and the transition away from PSTN as opportunities to work together and remove fraudulent traffic at source.

Overall, the session underlined that frontline fraud prevention relies on a combination of better signals, stronger partner relationships and shared infrastructure, with collaboration across the chain essential to move from isolated fixes to consistent, system wide protection.

Stop! Think Fraud Campaign

Speaker: Tamara Mauro-Trujillo - Home Office

This session provided an overview of the government's Stop! Think Fraud campaign, focusing on public attitudes to fraud, the behavioural barriers to self protection and the communications approach being used to shift perceptions and habits. It underlined the importance of consistent, practical messaging delivered through channels people already trust and use.

- **Understanding public attitudes to fraud:** Research presented showed that awareness of fraud as a risk is high and around 70 percent of people are concerned they could be affected. However, motivation to take protective action often remains low. Many still believe that only particularly vulnerable people are at risk, or that the sheer prevalence of fraud means becoming a victim is almost inevitable, which reduces the perceived value of preventative steps.
- **Clarifying what fraud looks like in practice:** A key challenge identified was that people often struggle to recognise fraudulent approaches in real time. The campaign therefore focuses on increasing understanding of common tactics and warning signs, and on encouraging people to pause, stop and think before responding. Normalising simple protective behaviours, such as setting up two step verification, is a central objective given that some still see it as time consuming or poorly understood.
- **Using a seasonal fraud calendar to stay relevant:** Tamara shared how the campaign plans activity across the year using a detailed calendar that aligns advice with real world moments. These include student loan payment dates, back to school periods, major sports tournaments and ticket sales, national cyber security and fraud awareness weeks, Christmas and Black Friday shopping peaks, and tax return deadlines. For each month, the team links these events to the fraud types most likely to surface at that time such as ticketing scams, recruitment and rental fraud targeting students, delivery and shopping scams, romance fraud around Valentine's Day and high pressure investment fraud. Social content, partner activity and campaign peaks are then mapped against this calendar so that advice feels timely and relevant rather than generic.
- **Reaching people where they are:** The session set out the multi channel strategy used to reach diverse audiences, including TV and video on demand, radio, outdoor advertising, social media and online platforms. Partnerships with media outlets and influencers, as well as organisations such as BT, Amazon and Starling, allow fraud prevention messages to be embedded in content and customer journeys that people already engage with, from sports coverage to ecommerce and banking apps.

- **Keeping advice engaging over time:** Looking ahead to 2026 and 2027, the campaign aims to keep messages fresh and closely aligned to evolving threats, using the calendar to sequence four major peaks around ticketing, romance, online shopping and delivery, and investment scams. This involves refining language, testing what resonates with different audiences and using real world examples linked to these peaks to illustrate both risks and practical steps.
- **Asks of industry and partners:** The Home Office invited organisations to share insight on threats, audiences and effective messaging, as well as to support the campaign through their own channels. Providers were encouraged to integrate Stop! Think Fraud prompts into customer journeys, co develop joint activities where appropriate and highlight further opportunities for collaboration so that consistent advice reaches consumers at scale.

The session made clear that Stop! Think Fraud is designed as a long term, behaviour focused campaign, with success depending on sustained industry support to embed simple, timely advice into the everyday interactions people have with banks, telecoms providers and online services.

Home Office Online Crime Centre

Speakers: Tracey Wright - CCUK, Justen Davis - Somos, Rod Lowson - Home Office, Paul Jacobus - Ofcom, Paul Morris - Vonage

This final session focused on the development of the Home Office's Online Crime Centre (OCC) and what a more integrated, data driven approach to online fraud and cyber crime could mean for the telecoms sector. Panellists discussed the OCC's role, early pilots, regulatory expectations and the practical steps needed to turn data sharing ambitions into operational reality.

- **Designing the Online Crime Centre as a system wide hub:** Rod Lowson outlined how the OCC, supported by significant government funding, is being built as a central hub for online fraud and high volume cyber crime that falls below the threshold of state sponsored activity. It brings together the Home Office, law enforcement, the intelligence community and private sector partners to pool data, analyse trends and coordinate interventions, with a strong emphasis on acting as early as possible in the fraud lifecycle.
- **From pilots to a single data sharing framework:** The panel heard about ongoing test and learn pilots, including work with telecoms, banks and technology platforms on SIM related fraud. These projects have highlighted both the complexity and the value of data sharing across sectors. The longer term ambition is to move toward a single, robust data sharing agreement, underpinned by legislation such as the Data Use and Access Act, to simplify participation for industry and support scale.
- **Insight, not just data, as the differentiator:** Paul Jacobus stressed that insight, rather than raw data alone, is often what unlocks progress. He illustrated how turning large volumes of fragmented information into structured intelligence can transform investigations, and gave examples of how regulatory changes around SIM farms and message routing can expand the scope for enforcement. The discussion reinforced the need for clearer visibility of which communications providers control which numbers, and for industry to move quickly on CP registries, numbering information and comprehensive Do Not Originate (DNO) lists in line with the fraud strategy.
- **International and cross sector coordination:** Justen Davis brought an international perspective, emphasising that most large scale fraud has cross border dimensions and that telecoms, finance and technology cannot tackle it in isolation. He argued that while it is not possible to address every issue at once, focusing on a small number of high impact capabilities such as interoperable traceback, trusted registries and well maintained DNO lists can significantly improve outcomes if implemented collaboratively and at pace.
- **Opportunities and responsibilities for industry:** Tracey highlighted the opportunity for CCUK members to help shape the evolving framework by contributing evidence to government calls for information and by sharing operational insight on what works in practice. The panel concluded that the OCC's success will depend on sustained public private partnership, with telecoms providers playing a central role in supplying high quality signals, participating in data sharing arrangements and aligning their own initiatives including CP registries, traceback and DNO implementation with the broader national effort to disrupt fraud at scale.

In closing, the session positioned the OCC as a key organising point for future fraud work, signalling that telecoms providers will be central partners in building a coherent data sharing ecosystem that underpins faster detection, stronger enforcement and better protection for the public.