Open call for evidence: Economic crime information sharing

Comms Council UK (CCUK) response

Consultation title	Economic crime information sharing
Full name	Ana Thompson Perea
Representing (individual/organisation)	Organisation
Organisation name	Comms Council UK (CCUK)
Email address	team@commscouncil.uk

About CCUK

1. Comms Council UK is a membership-led organisation that both represents and supports telecommunications companies that provide services to business and residential customers in the UK. We keep Britain talking in its various guises by providing or reselling voice services over data networks (VoIP) as well as other "over the top" applications including instant messaging and video.

2. The membership is a mixture of network operators, service providers, resellers, suppliers and consultants involved in a sector that is diversifying rapidly. CCUK represents its members at a policy level, builds coalitions to collaborate on industry initiatives and provides a platform to help members prepare for change, learn about new trends and develop new business relationships.

3. CCUK welcomes the opportunity to respond to this Call for evidence. Our response particularly focuses on the Private-Private, Private-Public and Cross-Border Information Sharing, and New Technologies sections.

General Comments

4. Fraud is cross-sector by design; criminals exploit gaps between telecoms, platforms, financial services, and law enforcement processes. Effective disruption therefore depends on timely proportionate, legally confident information sharing within the private sector, and with the public sector, including across borders.

5. Across CCUK's membership, and through the evidence gathered in CCUK's recent cross-sector data-sharing workshops organised with the Home Office, participants consistently highlighted that, for telecoms organisations, the legal environment for economic-crime information sharing is experienced as a complex patchwork of statutes, gateways, codes, exemptions, and sector-specific expectations. The volume

and fragmentation of relevant instruments creates uncertainty, drives risk-averse behaviour, and discourages proactive sharing even where it may be lawful and proportionate.

6. CCUK recommends that Government consider introducing clearer statutory protections (and clarity on associated regulatory enforcement risk) for disclosures made for economic crime purposes where an organisation has acted in good faith, on reasonable grounds, and in a proportionate manner, subject to appropriate safeguards (including data minimisation, audit trails, and governance controls). This should explicitly address scenarios involving immaterial or inadvertent over-disclosure when responding to authorised requests, which currently creates a chilling effect and undermines effective cooperation.

7. Even when lawful, information sharing often fails in practice due to inconsistent terminology and formats across different levels. For example, terminology varies significantly between the telecoms and financial sectors, and there is a lack of standardized data formats for specific signals - such as malicious SMS keywords - which forces providers into slow, bespoke bilateral agreements that SMEs struggle to negotiate. Furthermore, unclear points of contact between providers and the public sector that hinder collaboration, with law enforcement noting difficulty knowing who to contact within the telcos in the data-sharing workshops for example, while smaller providers often lack visibility into existing schemes and have no clear "route in" to share data. Finally, limited feedback loops prevent participants from seeing whether sharing "worked," which discourages long-term investment in these initiatives. There would be significant benefit in standardising data formats, terminology, and minimum operational expectations, and creating accessible routes into existing initiatives (with clear ownership and points of contact).

8. In order to strengthen fraud investigation and disruption, traceability must extend beyond the terminating network, as fraud investigation and disruption frequently requires visibility across the call chain and a model that relies too heavily on the terminating provider leaves systematic blind spots.

Responses to consultation questions

Chapter 1: Private-Private Information Sharing

Question 1: Economic Crime and Corporate Transparency Act 2023

1.1. Please describe your experience of sharing or receiving information with other private sector organisations for economic crime purposes using section 188 and 189 of the Economic Crime and Corporate Transparency Act 2023?

9. CCUK members in telecoms are generally not within scope of AML-regulated firm protections under ECCTA 2023 for private-to-private sharing. As a result, for many telecoms use cases, ECCTA provisions do not currently deliver the “confidence unlock” that AML-regulated sectors can benefit from.

10. In practice, this contributes to inconsistent private-to-private sharing across telecoms and adjacent sectors; delayed disruption, as signals arrive late or not at all; and

continued over-reliance on law enforcement requests, rather than earlier preventative action.

1.2. How could Government better support organisations share information with one another using section 188 and 189 of the Economic Crime and Corporate Transparency Act 2023?

11. Where ECCTA applies, Government support should focus on practical guidance on what "good" looks like (minimum necessary data, retention, audit trails), standardised formats and mechanisms (to avoid bespoke approaches), and clarity on liability and confidentiality boundaries alongside UK GDPR compliance.

1.3. What, if any, improvements should be made to section 188 and 189 of the Economic Crime and Corporate Transparency Act 2023? Please consider, for instance, whether more organisations should be bought into scope, whether new offences should be added to ECCTA 2023 or the technology and platforms for sharing.

12. CCUK supports consideration of expanding equivalent protections to non-AML regulated sectors, including telecommunications, where the purpose is preventing, detecting, or investigating economic crime/fraud and where appropriate safeguards are in place.

13. In particular, Government should address the current gap where AML-regulated sectors have clearer legal protections for private-to-private sharing, but telecoms and other non-AML sectors face greater ambiguity and perceived liability risk, despite holding high-value fraud indicators.

Question 2: Criminal Finances Act 2017

2.1. Please describe your experience of sharing or receiving information with other private sector organisations for economic crime purposes using Section 11 of the CFA 2017?

2.2. Please describe your perspective on the role of the Section 11 of the CFA 2017 information-sharing provisions now that Sections 189 and 199 of the Economic Crime and Corporate Transparency Act 2023 are in force?

2.3. What, if any, improvements should be made to Section 11 of the CFA 2017?

Question 3: General private-private sharing questions

3.1. Please describe your experiences of applying the Data Protection Act 2018 and UK GDPR when sharing or receiving information with other private sector organisations for economic crime purposes?

14. CCUK members report that legal uncertainty is a primary barrier to effective private-to-private sharing, even where the intent and public interest are clear. Common issues include uncertainty over lawful basis and the applicability of exemptions in fast-moving fraud scenarios, concerns that sharing outside a strict statutory gateway

may be viewed as unlawful disclosure, and over-compliance and defensive decision-making, particularly among smaller providers.

3.2. Please describe the impact that the Data (Use and Access Act) 2025 will have on how organisations share or receive information with other private sector organisations for economic crime purposes?

15. CCUK recognises that DUAA 2025 may offer additional clarity and reassurance in some scenarios. However, members' expectation is that DUAA alone does not provide enough reassurance and there still remains persistent ambiguity about "who can share what with whom" in telecoms fraud use cases. Therefore, although helpful, it remains insufficient without sector-specific guidance which acknowledges that data-sharing in good faith should not cause regulatory risks to members, as well as templates from Government.

3.3. How else could Government better support private-private information sharing for economic crime purposes?

16. CCUK recommends Government prioritise:
    a. Telco-specific lawful sharing guidance with worked examples.
    b. A proportionate compliance framework for SMEs, including minimum expectations and template agreements.
    c. Standard terminology and data formats to reduce friction and increase scalability.
    d. Clear mapping and signposting of existing initiatives and points of contact.
    e. Feedback loops so participants understand the impact/value of sharing (to sustain engagement and justify investment).
    f. Good-faith protections (with governance) to enable earlier intervention.

Chapter 2: Private-public questions (for all)

Question 4: Financial intelligence gateway and pre-order enquiries

4.1. Please describe your experience of sharing or receiving information via the Financial Intelligence Gateway, or in pre-order enquiries in advance of a production order, for economic crime purposes?

4.2. Could Government introduce improvements to the way information is shared via the Financial Intelligence Gateway or in pre-order enquiries in advance of a Production Order?

Question 5: Proceeds of Crime Act 2002 Part 8

5.1. Please describe your experience of sharing or receiving information in response to a Part 8 Proceeds of Crime Act 2002 Order (Production Orders, Disclosure Orders, Unexplained Wealth Orders, Customer Information Orders and Account Monitoring Orders)? Please feel able to comment on all or specific orders.

5.2. Please consider how Government could improve or better support sharing of information in response to a Part 8 Order (Production Orders, Disclosure Orders, Unexplained Wealth

Orders, Customer Information Orders and Account Monitoring Orders)? Please feel able to comment on all or specific orders.

17. Where information is requested by competent authorities, CCUK members' priority is clear scoping, secure transmission, and assurance that compliance in good faith will not create disproportionate regulatory exposure. Clear scoping should be defined by the following principles:
    a. Precise temporal and data boundaries, with requests strictly limited to the specific timeframe and data points required for the investigation to prevent inadvertent over-disclosure.
    b. Operational feasibility, accounting for the diverse technical architectures of different networks and with guidance that includes "worked examples" of what data points are legally and technically permissible to share.
    c. Standardised request formats aligned across different sectors to reduce risk of misinterpretation.
    d. Explicit regulatory assurance for providers acting in good faith to fulfil a request.
    e. A proportionate compliance framework for SMEs, including minimum expectations.

Question 6: Crime and Courts Act 2013

6.1. Please describe your experience of sharing or receiving information with the NCA using Section 7 of the Crime and Courts Act 2013?

18. Members generally consider law-enforcement-led sharing routes clearer than private-to-private sharing, largely because the requestor's authority is clearer, processes are more established, and the perceived lawful basis is more explicit.

6.2. Should a similar gateway to Section 7 of the Crime and Courts Act 2013 be available to other public bodies and, if so, which public bodies?

19. CCUK considers that more clarity around what "public bodies" include is needed in order to assess safely.

20. Any expansion must include a clear, tightly scoped definition of eligible bodies, explicit purpose limitations and safeguards, and transparency about oversight, misuse prevention, and proportionality.

Question 7: Suspicious Activity Reporting

7.1. Noting recent improvements to the Suspicious Activity Reporting regime, please describe your current experiences of sharing or receiving information through Suspicious Activity Reporting in Part 7 of the Proceeds of Crime Act 2002?

21. Telecoms providers often observe activity that is suspicious or harmful, but which does not neatly map onto AML-focused SAR regimes. Members' experience demonstrates that much telecoms fraud intelligence is not readily reportable via SARs without uncertainty about scope and thresholds.

7.2. What further changes, if any, could be made to the Suspicious Activity Reporting regime to make it more effective in delivering its objective to provide high value intelligence to law enforcement?

22. CCUK recommends clearer guidance on: when SARs are relevant outside traditional AML scenarios, what constitutes "reportable suspicion" for fraud typologies observed in telecoms, and how SAR reporting should intersect with other reporting pathways to avoid duplication.

7.3. With the growth of public-private partnerships and real-time data sharing such as Data Fusion, please describe your perspective on the role, utility and value-add of the Suspicious Activity Reporting regime?

23. CCUK supports the principle that SARs should focus on unique value-add. Where faster, targeted sharing mechanisms exist (or can be built) for telecoms fraud, SARs should not become the default "catch-all" route that increases burden without improving disruption outcomes.

7.4. What benefits or risks, if any, would there be to changing the suspicion threshold to 'reasonable grounds to suspect' in the Suspicious Activity Reporting regime and would you support this change?

24. CCUK emphasises that any threshold change must be assessed for impact on reporting volume and burden and whether it meaningfully improves actionable intelligence.

Question 8: Investigatory Powers Act 2016 and related amendments

8.1. Please describe your experience of acquiring or sharing communications data under the Investigatory Powers Act 2016, including any related amendments, for economic crime purposes?

25. CCUK members described that IPA processes can be workable when appropriately scoped. However, experiences vary, and the ecosystem often appears overly focused on the terminating network, limiting investigative visibility.

26. A key concern to take into account is that providers can be placed in a difficult position where strict compliance is expected but fear of minor error (or perceived over-disclosure) can damage trust and willingness to cooperate.

8.2. Please consider how Government could improve or better support the acquisition of communications data under the Investigatory Powers Act 2016, including any related amendments, for economic crime purposes?

27. CCUK recommends:
    a. Stronger traceability mechanisms that support investigation beyond the terminating provider and capture the full call chain where proportionate.
    b. Consistent training/standards for requestors, to reduce inappropriate scoping and ensure requests are precise and operationally feasible.
    c. Good-faith protections to prevent disproportionate consequences where a provider acts reasonably to assist (including inadvertent immaterial over-disclosure).
    d. Greater clarity on what "best practice" looks like in telecoms fraud cases—especially for SMEs.

Question 9: General public-private sharing questions

9.1. Please describe your experiences of applying the Data Protection Act 2018 and UK GDPR when sharing information or receiving information owned by the private sector with law enforcement for economic crime purposes?

28. Members generally find law enforcement requests clearer than private-to-private sharing, because the lawful basis and authority are more explicit.

29. Often fear of repercussions for small mistakes such as minor inadvertent over-disclosure leading to escalation / reporting undermine trust and deter proactive cooperation.

9.2. Please consider how else Government could better support information-sharing between public and private bodies for economic crime purposes?

30. CCUK recommends publishing clear, telco-specific guidance on handling law enforcement requests (including scoping, minimisation, retention, audit trails); standardising request formats and secure transmission; creating clear escalation routes for resolving uncertainty without penalty; and introducing proportionate good-faith protections to avoid chilling effects.

Chapter 4: Cross-border sharing (all)

Question 11: General cross-border information sharing question

11.1. Please describe your experience of sharing or receiving information cross-border for economic crime purposes?

31. CCUK members' experience demonstrates limited coordination operationally, and cross-border sharing being materially harder than domestic sharing. Challenges include compounded legal risk across multiple jurisdictions, uncertainty about what can be shared with whom (and under what authority), and difficulty aligning UK needs with providers subject to non-UK legal constraints.

11.2. How could Government improve or better support the sharing of information cross-border for economic crime purposes?

32. CCUK recommends clear signposting of available routes for cross-border cooperation in telecoms fraud cases (including practical "how to" playbooks); working to improve speed and interoperability of lawful cross-border mechanisms for time-sensitive fraud disruption; publishing guidance that recognises real-world constraints for global providers (including conflicts-of-law concerns); and promoting international collaboration specifically focused on telecoms traceability and fraud signal sharing, to reduce reliance on slow, fragmented processes.

New technologies

Question 12: New technologies

12.1. How could Government best optimise the growth of new technologies such as automation or artificial intelligence to support the public sector and private sector to detect and act upon information related to economic crime? Please share detail of the technology, its benefits, risks and any operational or legislative considerations.

33. CCUK supports a regulatory environment that enables proportionate use of advanced technology to counter criminals who are already innovating rapidly.

34. AI-driven fraud detection on voice traffic needs to: be enabled in a way that does not require "wiretap-style" human monitoring; focus on signals and scam profiles rather than indiscriminate recording; is triggered by risk indicators (e.g., traffic spikes, short durations, abnormal error patterns); and is governed by privacy-by-design, minimisation, and strong oversight.

35. Government should clarify and (where needed) reform rules so that providers can lawfully deploy privacy-preserving, risk-based AI analysis to detect scam voice activity, recognising that fraudsters "channel hop" - scams are moving from SMS to Text-to-Speech APIs, then to MP3 files, and finally to streaming audio - and adapt quickly to evade controls.

36. CCUK also notes the increasing relevance of data sovereignty and regionalisation pressures, and customer-imposed restrictions on where data/signals can be processed, which can complicate global-scale deployment of counter-fraud tooling. Global platforms face pressures where customers mandate data cannot leave certain regions, which complicates a unified global fraud response.

37. Government should ensure that future policy supports secure innovation while acknowledging these operational realities.

Anything else

Question 13: Any other areas

13.1. Are there any other areas not covered by the above 1-12 questions that could be addressed to improve economic crime information sharing?

38. CCUK welcomes this consultation given the important role data sharing plays in protecting customers. However, data sharing is only one part of the solution, which needs to work together with other regulatory interventions through an integrated approach to effectively disrupt complex fraud chains. These interventions / solutions include:
    a. Traceback solutions: CCUK welcomes the Home Office's advocacy for traceback capabilities. Currently, the manual process to work back up the chain to find a call source is rarely used and seldom produces results due to complexity and data sharing concerns. We support a semi-automated solution, similar to the model mandated in the USA, where each party notifies the next provider in the chain to quickly identify and challenge the true source of a call.
    b. A CP register: There is an urgent need for an industry-wide register of Communications Providers supported by a secure, authenticated messaging network. This infrastructure is required to facilitate rapid, coordinated responses and enable trustworthy information sharing between verified participating organisations.

c. A numbering repository: current investigations remain slow because there is no automated way to identify which service provider is responsible for a telephone number. CCUK proposes a standardised API and web portal driven network to interrogate numbering data across the supply chain in real-time.

39. The industry requires a trusted mechanism that accommodates this multi-faceted approach to accommodate the complexities of the modern communication supply chain