Sharing data to tackle fraud: Supporting documentation

Appendix 1 – Why data sharing is permitted

Data protection law shouldn't be seen as creating a barrier to sharing data for fraud prevention so much as providing a framework for doing so responsibly. Many providers incorrectly assume that the legal framework prevents fraud-related information sharing. In practice, UK data protection law can support lawful sharing for the prevention and detection of crime and for protecting customers and organisations. The UK GDPR, the Data Protection Act 2018 (DPA 2018) and the Data Use and Access Act 2025 (DUAA) provide the legal basis for this - see Appendix 2.

Where organisations have acted in good faith, on reasonable grounds, in a proportionate manner, and in accordance with data protection legislation, the approach of UK regulators and enforcement bodies is to support compliant sharing rather than penalise it.

Government commitments to data sharing: Data sharing for fraud prevention sits at the heart of the UK government's Fraud Strategy 2026–2029. It explicitly commits to "collaborating with online intermediaries, financial platforms and service providers to share data and jointly block criminal activity at scale" and to launching the Online Crime Centre (OCC) as a "public-private data sharing hub to support joint interventions against online fraud." Under the voluntary Telecommunications Fraud Charter (November 2025) signed by CCUK, CCSG and the Home Office, signatories committed to "create a seamless, multi-sector data-sharing ecosystem that enables faster detection of bad actors". The Home Office recently published a Call for Evidence on how data is currently shared for detecting, preventing, investigating, or disrupting economic crime, and how the system could be improved.

We want organisations to approach data sharing for fraud prevention by looking for why they can share, rather than defaulting to reasons why they cannot. The legal framework provides a strong foundation. The guidance in this document is designed to give you the confidence to share data lawfully, proportionately, and help disrupt fraud.

Appendix 2 - The legal framework

A number of laws and regulations are relevant to data sharing for fraud prevention in the UK. This is not an exhaustive legal guide and organisations should seek their own legal advice where needed and consult the ICO's guidance resources linked in Section 7.

- **UK General Data Protection Regulation (UK GDPR)**: The core framework governing lawful sharing of personal data. Fraud prevention can constitute a "legitimate interest" or "public task" under the UK GDPR.
- **Data Protection Act 2018 (DPA 2018)**: Governs lawful processing of personal data including law enforcement purposes. Section 2.1.2 provides a gateway for sharing data for the prevention and detection of crime or the apprehension of offenders. Law enforcement exemptions derive from Part 3.
- **Data Use and Access Act 2025 (DUAA 2025)**: Under the DUAA 2025, the prevention of crime (including fraud) is a "recognised legitimate interest". This new framework has removed the need for a proportionality test or a Legitimate Interest Assessment (LIA). However, retention of the term 'necessary' means organisations must decide and evidence that they believe data sharing will contribute to prevention of fraud. The guidance should outline this new framework as an opportunity, rather than a legal hurdle to overcome.
- **Crime and Courts Act 2013**: Provides a statutory gateway for sharing information with the National Crime Agency (NCA), underpinning public-private intelligence sharing such as JMLIT.
- **Criminal Finances Act 2017**: Supports private-to-private data sharing for economic crime purposes, providing a basis for sharing between telecoms providers, banks, and other private sector organisations.
- **Serious Crime Act 2007**: Section 68 designates "Specified Anti-Fraud Organisations" (SAFOs) – bodies such as CIFAS and TUFF which have specific powers to share fraud data between members. Section 85 provides a further information-sharing gateway linked to proceeds of crime
- **Economic Crime and Corporate Transparency Act 2023 (ECCTA 2023)**: Enables information sharing between anti-money laundering (AML) regulated firms and enhances Companies House powers. Relevant where telecoms providers interact with AML-regulated partners.
- **Investigatory Powers Act 2016 (IPA 2016)**: Provides the framework for lawful acquisition of communications data for crime prevention and investigation. Note: This applies primarily to law enforcement requests – non-law enforcement bodies (such as CDA) rely on DPA provisions instead.
- **Proceeds of Crime Act 2002 (POCA)**: Establishes the Suspicious Activity Reports (SARs) regime and information powers relating to money laundering and asset recovery.
- **The Privacy and Electronic Communications Regulation**: Sits alongside the DPA and UK GDPR to govern electronic marketing, web cookies and customer data privacy.

Specified anti-fraud organisations (SAFOs): Sharing through Specified Anti-Fraud Organisations (SAFOs) under section 68 of the Serious Crime Act 2007 provides additional legal certainty. In the telecoms space, the key SAFOs are:

- **CIFAS**: a not-for-profit organisation operating the National Fraud Database (NFD), the UK's largest cross-sector fraud prevention database, with 800+ members across banking, insurance, telecoms, retail, utilities, and the public sector. In 2025, 444,000 cases were filed; members reported £2.1 billion in recorded savings.
- **TUFF** (Telecommunications UK Fraud Forum): a SAFO specifically for the telecoms sector. Provides fraud intelligence sharing, training, and coordination with National Trading Standards, Communications Fraud Control Association (CFCA), and law enforcement.

Appendix 3 - Additional guidance and resources

Key ICO documents

- **The Data Use and Access Act 2025 (DUAA) - what does it mean for organisations?**: The ICO's practical explainer on how the DUAA changed data protection law, including its implications for legitimate interests processing. It outlines specifically that the DUAA amended, but did not replace, the UK GDPR, the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications Regulations (PECR).
- **Data protection is not an excuse when tackling scams and fraud**: The ICO's statement making clear that data protection law should not be used as a reason to avoid sharing information for fraud prevention purposes.
- **Information security guidance**: Practical guidance on keeping personal data secure, aimed at smaller organisations. Relevant for providers who want to share data but are uncertain whether their security arrangements are sufficient.
- **Sharing personal information when preventing, detecting and investigating scams and frauds**: The ICO's primary guidance for private-sector organisations on sharing personal information with each other to support fraud mitigation. Sets out requirements including: carrying out a data protection impact assessment; being clear about responsibilities; setting up data sharing agreements; identifying a lawful basis for sharing; understanding the type of information being shared; complying with data protection principles; and respecting people's rights.
- **Data Sharing Code of Practice**: The ICO's statutory code of practice on data sharing, which provides detailed guidance on how to share personal data in compliance with UK GDPR and DPA 2018. Covers data sharing agreements, data protection impact assessments, and transparency.
- **Legitimate Interests Guidance**: Guidance on using legitimate interests as the lawful basis for processing, including how to conduct a legitimate interests assessment (LIA). Particularly relevant for private-to-private data sharing where another explicit gateway may not apply.
- **Recognised Legitimate Interest Guidance:** Guidance on the "recognised legitimate interest" lawful basis introduced for handling personal information.
- **Law Enforcement Processing**: Guidance on processing personal data for law enforcement purposes under Part 3 of the DPA 2018. Part 3 does not apply to telecoms providers themselves; it governs the competent authorities (such as law enforcement bodies) with whom data may be shared. This guidance helps providers understand the rules those bodies operate under.
- **Advice and services (ICO):** Where an issue is particularly complex or requires detailed consideration, organisations can use the ICO's advice and services — including its business advice service — to seek further reassurance.

Note: some ICO guidance is currently being updated to reflect the DUAA 2025. Check the ICO's plans for new and updated guidance for the latest information.

Ofcom guidance on preventing misuse:

- **Good practice guide to help prevent misuse of sub-allocated and assigned numbers**: Guidance on due diligence checks before sub-allocating or assigning numbers, ensuring continued compliance and reassessing risk; and responding to incidents of misuse.
- **Calling Line Identification (CLI) guidance**: Guidance on the provision and appropriate use of CLI, including in relation to the accuracy and presentation of numbers
- **Guidance on scam mobile messages**: Guidance on scam mobile messages: Practical guidance for providers on identifying and responding to scam mobile messages. [Note: Final version but not in force until 2027]
- **Persistent Misuse Statement**: Ofcom's statement on persistent misuse of electronic communications networks and services, setting out the different forms of misuse and Ofcom's powers to identify and take action against misuse.
- **Guidance on preventing misuse of global titles**: Rules and guidance on preventing misuse of global titles: rules banning leasing of global titles in SS7 signalling and guidance for number range holders to prevent misuse of global titles.
- **Telecoms numbering guidance**: Ofcom's general guidance on telecoms numbering, including obligations on providers holding or using number ranges.

Appendix 4 - Real-world examples of successful data sharing

SMS Blasters initiative

One was identified in the UK through analysis of 7726 reports[1], when it was noticed that there were no records of the messages on the mobile network. Detection was possible because the main MNOs and the ICO have reciprocal access to each other's data — this access was instrumental to the SMS Blaster work.

NCSC pulled together a cross-industry team - comprising NCSC, Ofcom, the main MNOs, the Dedicated Card and Payment Crime Unit (DCPCU), and City of London Police - to share the findings. Two of the MNOs worked closely with local police units to track the origin of the device. This led to the identification of a suspect vehicle and the arrest of the driver while they were in the process of sending messages. The driver has since been convicted and sentenced.

This is an example of what cross-sector collaboration makes possible - none of the organisations involved could have achieved this outcome alone.

UK Blocked SIMs Programme

PAYG SIMs were identified as being systematically diverted in bulk from legitimate UK retail distribution channels. The SIMs were never registered, charged, or used to make calls — but they were receiving One-Time Passcodes that were being used to create online accounts at scale, including social media, dating and messaging platforms. Some of those accounts were then used to scam UK consumers.

UK telecoms providers identified the diverted SIMs and blocked numbers that breached their terms and conditions. The associated online accounts, however, remained active. To address this, telecoms providers worked with Stop Scams UK to share the blocked numbers — lawfully and safely — with online platforms and financial services providers, enabling them to identify and act on potentially fraudulent accounts linked to those numbers.

The result is a coordinated cross-sector response that has introduced a financial friction into PAYG SIM usage and significantly reduced fraud through this route. The programme has also become genuinely reciprocal: online platforms and financial services providers now return associated data — such as additional phone numbers or email addresses — to telecoms companies, widening the net further. Previously undetected fraudsters are being identified and blocked before they can move across multiple channels to reach potential victims.

The Blocked SIMs programme demonstrates that data originating with telecoms providers can unlock cross-sector solutions — and that data sharing can evolve into a live, two-way ecosystem rather than a one-time disclosure.

[1] Note: the 7726 service is fronted by Mobile UK and run by Proofpoint on behalf of the MNOs — not all MNOs currently support it

Telco-Bank Fraud Intelligence Sharing

The CDA, along with two telco providers, were able to share data with financial institutions for the purposes of identifying potential victims of fraud. When a number of calls were made impersonating a bank in order to fraudulently extract funds, the comms provider was able to identify the businesses targeted by the caller. Banks were then able to investigate with those customers and add additional fraud monitoring and controls.

Appendix 5 - Data-sharing case studies

Organisation details:	
Organisation:	Cyber Defence Alliance (CDA)
Type of organisation:	Not-for-profit
Data-sharing initiatives:	
Name of the project or data stream:	Malicious Domains
Current status (past; ongoing/live; or future/in the process of setting it up)	Live
Partner organisation (who the data is shared with):	Multiple, including GASA, GSE, Google, mobile network operators, ISPs, NCSC (UK/IE); blocklists' some Registrars & Hosters and browser protection organisations
Type of agreement (formal DSA, informal, via email complying with GDPR etc)	Data sharing agreements with some although informal agreements with some others. DPIA completed.
Primary objective (type of fraud it aims to stop):	To identify malicious domains and websites used by Threat Actors (TAs) for criminal purposes, including defrauding victims through false payments and data theft, OTP capture, downloading remote access tooling, malware hosting/infection, and/or C2 infrastructure. These are identified and confirmed as 100% malicious by the CDA then sent to telco partners listed above (all main MNOs) and other partners for mitigations. MNOs will block customers from accessing these domains at the DNS level.
Data points shared:	Domains (not sub domains)
Direction of flow (e.g. telco -> organisation -> bank):	CDA data hunt AND sharing from members, wider FS, and other partners CDA triage and assessment for accuracy (True Malicious) share high confidence malicious domains to partners (per above list)

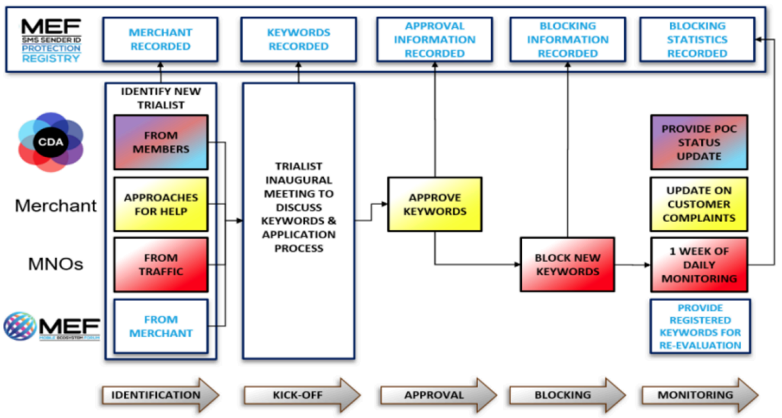
	
Volume and frequency of data:	Daily (plus more frequent hunting for specific high-harm campaigns) Volume: 2,000-5,000 per day for long list. Triage process typically reduces to 100-400 per day for mitigation that are high confidence (as close to 100%) sharing. 100,000s have been shared over the last 6 years.
Impact/metrics (if available)	
Number of victims protected	Millions
£ value saved	Millions of GBP
Number of "bad actors" identified	This work led to the identification of threat actors who ran criminal services such as Labhost that allowed fraudsters to set up fake websites on newly created domains and direct phishing traffic to those sites. The CDA identified the main indivduals behind these criminal services – he received over 8 years in prison and around 140 arrests globally of fraudsters using that site, Site and database seized by law enforcement.
Qualitative impact	CDA data feed is widely accepted as best feed within the Share & Defend programme in terms of confidence to act upon data. Our volume is lower than some other feeds but the additional automated and manual assessments undertaken *prior to* sharing means recipients are able to act/block without conducting their own analysis, saving time and resourcing across the multiple end users of the data. By following specific and significant campaigns, CDA are also able to focus on HIGH HARM domains, meaning that those that are more likely to result in significant losses (either low volume-high value

	individual losses e.g. business frauds through the remote access; or low value-high volume mass losses to sophisticated campaigns, e.g. winter fuel payments).

Organisation details:	
Organisation:	Cyber Defence Alliance (CDA)
Type of organisation:	Not-for-profit
Data-sharing initiatives:	
Name of the project or data stream:	Fraudulent telephone number takedown
Current status (past; ongoing/live; or future/in the process of setting it up)	Ongoing effort: widely supported across telco sector. All UK MNOS support this and additionally dozens of VOIP and other such providers.
Partner organisation (who the data is shared with):	CDA and Telco providers (all MNO and a VOIP provider to date only).
Type of agreement (formal DSA, informal, via email complying with GDPR etc)	Data sharing agreement, DPA 2018 (2.1.2) with one MNO and other shared via DPA legislative gateway but no formal agreement.
Primary objective (type of fraud it aims to stop):	To take telephone numbers out of use which are being used for fraudulent purposes eg. Calling victims; sending SMS lures; impersonating banks etc.
Data points shared:	Telephone numbers.
Direction of flow (e.g. telco -> organisation -> bank):	Case study summary: Threat Actors engaged in fraud by calling victims or sending them an SMS lure or similar with a telephone number in the lure requesting the victim calls them. By taking this telephone number out of use prevents victims from contacting, unsuspectingly, the fraudster. Flow: Telephone number identified by Bank being used in numerous Fraud cases shared to CDA CDA identifies owning network/org then submits request for telephone takedown Telco removes that

	telephone number from use
Volume and frequency of data:	1,275 were taken out of use in the fourth quarter of 2025. 300 – 400 per month however continues to grow.
Impact/metrics (if available)	
Number of victims protected	100s or 1000s each month
£ value saved	Significant – these frauds average loss is around 10000s of £s with some much higher
Number of "bad actors" identified	
Qualitative impact	These timely submissions are disrupting these fraudsters – often mid call, from operating.

Organisation details:	
Organisation:	Cyber Defence Alliance (CDA)
Type of organisation:	Not-for-profit
Data-sharing initiatives:	
Name of the project or data stream:	SMS Blocking
Current status (past; ongoing/live; or future/in the process of setting it up)	POC-Live
Partner organisation (who the data is shared with):	MEF. Initial POC testing by Vodafone looking for abuse of Barclays brand/customers however now expanded to include Vodafone-Three & BT/EE are putting this is place also. TSB and Co-operative Bank now also participate.
Type of agreement (formal DSA, informal, via email complying with GDPR etc)	Data sharing agreements, DPIA completion, formal agreements
Primary objective (type of fraud it aims to stop):	To identify SMS malicious messaging that abuses legitimate branding to convince victim to click on a link, continue a message conversation, or make a call to the Threat Actor (TA). Primary

	objective for the fraudsters is to defraud victims through fraudulent payments and/or collecting further security information that would allow account takeover/digital wallet frauds or similar. Secondary purpose: malware infections, other personal data theft
Data points shared:	Malicious SMS samples; keywords/phrases that banks use to identify legitimate traffic and keywords/phrases that the fraudsters use to identify malicious SMS purporting to be from the bank. This can be programmed into the SMS Firewall/Spam Shield to detect malicious campaigns.
Direction of flow (e.g. telco -> organisation -> bank):	POC phase: Malicious messaging identified via victim reporting to banks and telcos shared to org for assessment against keywords/phrases used in legitimate communications org confirms keywords that are malicious (not used legitimately) sent to telco for learning and blocking future campaigns Once in production: MEF will hold and update lists of 'malicious keywords and act as conduit with telcos. Full process flow 
Volume and frequency of data:	Operational work has commenced with weekly meetings to identify new keywords used within messages and to tweak blocking controls and discuss any issues raised. Plans to expand this work across additional banks/brands and mitigation partners.
Impact/metrics (if available)	
Number of victims protected	100,000s
£ value saved	
Number of "bad actors" identified	

Qualitative impact	Over 600K malicious SMS messages blocked from reaching customers of participating telco that are purporting to be from the participating bank within 5 months. Continues to be expanded.

Organisation details:	
Organisation:	Cyber Defence Alliance (CDA)
Type of organisation:	Not-for-profit
Data-sharing initiatives:	
Name of the project or data stream:	FS-Telco sharing: Call Data (and associated customer details)
Current status (past; ongoing/live; or future/in the process of setting it up)	Ongoing effort: occasionally achieved.
Partner organisation (who the data is shared with):	CDA and two Telco providers (a MNO and a VOIP provider to date only
Type of agreement (formal DSA, informal, via email complying with GDPR etc)	Data sharing agreement, DPA 2018 (2.1.2) with one MNO and other shared via DPA legislative gateway but no formal agreement.
Primary objective (type of fraud it aims to stop):	To utilise provisions available via Data Protection Act 2018 (2.1.2) (for the prevention and detection of crime and/or the apprehension of offenders) to: Share intelligence that may result in identifying potential / future victims of fraud (and possibly also the offenders), and to share this data to financial institutions for relevant investigation, monitoring and/or mitigation controls. Primary objectives are: 1. to protect victims known to have been subject to contact via vishing by threat actor(s) aiming to cause significant losses 2. where a fraud has occurred, to identify cases linked to specific campaign(s) and threat actor(s) for purposes understanding scale and impact, and identifying intelligence opportunities.
Data points shared:	Telephone numbers, call data.
Direction of flow (e.g.	Case study summary:

telco -> organisation -> bank):	Threat Actors engaged in fraud against businesses/customers by calling them to impersonate banks in a bid to fraudulently extract funds. Once the suspect phone number used consistently for vishing calls was identified call data is requested to identify the victims. Request sent to the MNO for call data associated to number. Response received and phone numbers assessed to identify associated businesses. Business names shared to member banks for protection and/or fraud investigations. Over 400 victims protected in one case alone. Flow: Telephone number identified by Bank being used in numerous Fraud cases shared to CDA CDA submits request for call data under DPA 2.1.2 response received with called numbers CDA research to identify associated businesses Business names shared to banks for investigation and protection controls
Volume and frequency of data:	Very infrequent.
Impact/metrics (if available)	
Number of victims protected	491 businesses identified being called by number known to be attempting vishing. Disseminated to banks for monitoring and/or investigation. Data not available on how many of these businesses had fraud, or frauds prevented due to this dissemination.
£ value saved	Significant – these frauds average loss is around £30,000 with some much higher
Number of "bad actors" identified	1 to date via this method
Qualitative impact	Very high value losses are associated to this fraud type, which is being conducted at scale by several sophisticated Threat Actor Groups (though specific losses in this case are unknown).

Organisation details:	
Organisation:	Cyber Defence Alliance (CDA)
Type of organisation:	Not-for-profit
Data-sharing initiatives:	
Name of the project or data stream:	FS-Telco sharing: Actionable Intelligence Sharing (PII)

Current status (past; ongoing/live; or future/in the process of setting it up)	Ongoing effort: occasionally achieved.
Partner organisation (who the data is shared with):	CDA & VoiceHost
Type of agreement (formal DSA, informal, via email complying with GDPR etc)	Informal agreement, Responsible disclosure, DPA 2018 (2.1.2) request for data submission
Primary objective (type of fraud it aims to stop):	To utilise provisions available via Data Protection Act 2018 (2.1.2) (for the prevention and detection of crime and/or the apprehension of offenders) to: Build an actionable intelligence picture of fraud campaigns that highlight the nature, scale and impact of offending(s) and identifies where intelligence may be held that leads to the real-world identity of offenders, or can lead to the identification of offenders through Law Enforcement (LE) legal gateway enquiries. Note: proportion, necessity and collateral intrusion are fully considered for all such enquiries under DPA provisions.
Data points shared:	PII data including: names, telephone numbers, email addresses, physical addresses, online handles (usernames). Details associated to offending, including financial data, bank accounts and transactions.
Direction of flow (e.g. telco -> organisation -> bank):	Case study summary: The CDA operate a 'telco abuse report' provision whereby banks who receive testimony from customers on attempted/actual telephony based social engineering can share into the CDA for onward dissemination to network providers, who can investigate for abuse and take necessary action. One such smish-to-vish report was submitted by a CDA member. VoiceHost (the providing network) undertook investigations and identified intelligence that could assist in developing the picture of offending and opportunities for attribution. This data was shared into the CDA. The CDA developed this information, and further intelligence shares with members led to the identification of multiple victims of this campaign as well as significant opportunities for attribution to a real-world identity. Intelligence is now submitted to Law Enforcement for investigation. Flow:

	Smish-to-vish message shared by customer to Bank Bank shared to CDA CDA abuse report shared to VoiceHost VoiceHost responsible disclosure of intelligence shared to CDA intelligence development by CDA and DPAs shared to members results received by CDA and intelligence package created for LE
Volume and frequency of data:	Very infrequent.
Impact/metrics (if available)	
Number of victims protected	
£ value saved	
Number of "bad actors" identified	
Qualitative impact	At least nine victims have been identified, including vulnerable customers. This is an excellent example of where data held in different organisations can be shared to attribute offending and to understand the true nature and scale of offending across organisations.

Organisation details:	
Organisation:	Cifas
Type of organisation:	Not for profit, Specified Anti- fraud Organisation (as stated in s68 Serious Crimes Act 2007)
Data-sharing initiatives:	
Name of the project or data stream:	1) National Fraud Database (NFD) 2) Insider Threat Database (ITD) 3) Vision 4) APP Victim Check Database 5) Intelligence Service 6) Peer to Peer Services
Current status (past; ongoing/live; or future/in the process of setting it up)	1 & 2 Ongoing 3 - 6 are new services with increasing membership over time
Partner organisation (who the data is shared with):	800+ members across NFD/ITD; Banking and financial services, insurance, telecommunications, retail, utilities, public sector and local authorities

Type of agreement (formal DSA, informal, via email complying with GDPR etc)	Formal membership agreement for NFD, supplementary agreements for other services
Primary objective (type of fraud it aims to stop):	Identity fraud which enables investment, romance and other scam typologies, facility takeover, misuse of facility, application fraud, asset finance and insurance claims
Data points shared:	Name, DoB, address, telephone, email, IP address, facial images, financial accounts data,
Direction of flow (e.g. telco -> organisation -> bank):	Member – Cifas – member
Volume and frequency of data:	2 million active cases in the NFD 444,000 cases filed in 2025. 1000 plus cases in the ITD 200 + cases filed in 2025
Impact/metrics (if available)	
Number of victims protected	
£ value saved	Members reported savings of £2.1 billion in recorded savings
Number of "bad actors" identified	
Qualitative impact	

Organisation details:	
Organisation:	NTS Scams Team
Type of organisation:	Trading Standards (Law enforcement)
Data-sharing initiatives:	
Name of the project or data stream:	PUULA
Current status (past; ongoing/live; or future/in the process of setting it up)	Ongoing development – Requires next steps
Partner organisation (who the data is shared with):	CCUK/TUFF/NICC

Type of agreement (formal DSA, informal, via email complying with GDPR etc)	Semi formal. With an MOU and data capture standards Results exchanged via email – GDPR and IPA compliant
Primary objective (type of fraud it aims to stop):	Mass marketing and investment frauds (includes green energy, housing disrepair, claims management and debt
Data points shared:	CLI's, traffic levels and where available end users of the number/service
Direction of flow (e.g. telco -> organisation -> bank):	Telco -NTS and Reverse
Volume and frequency of data:	Currently in low figures as currently a manual pilot. Further work being undertaken to escalate to a digital/API system (Funding requirement)
Impact/metrics (if available)	
Number of victims protected	Exact figures not calculated. Estimated at in excess of 10,000
£ value saved	£4 million est, since inception based on detriment saved by UK consumers (Can provide more detail)
Number of "bad actors" identified	As of Feb 26 – 39 OCG type fraud entities
Qualitative impact	Situationally vulnerable victims are not targeted by these calls

Organisation details:	
Organisation:	Information Commissioner's Office (ICO)
Type of organisation:	The ICO is the UK's independent regulatory body in respect of data protection, freedom of information, privacy and electronic communications, and environmental information regulations.
Data-sharing initiatives:	
Name of the project or data stream:	Unsolicited direct marketing texts and calls by organisations in relation to motor finance claims in contravention of the Privacy and Electronic Communications Regulations (PECR).
Current status (past; ongoing/live; or future/in the process of	Ongoing/live

setting it up)	
Partner organisation (who the data is shared with):	Other relevant regulators
Type of agreement (formal DSA, informal, via email complying with GDPR etc)	• Memorandum of Understanding (MOU) • S132 Data Protection Act 2018
Primary objective (type of fraud it aims to stop):	To share relevant information to assist ICO and partner organisations in progressing relevant investigations.
Data points shared:	
Direction of flow (e.g. telco -> organisation -> bank):	Data is shared both ways between partner organisations.
Volume and frequency of data:	Regular meetings held to discuss and share information regarding investigations in this area.
Impact/metrics (if available)	
Number of victims protected	Our PECR investigations are proactive and based on the number of complaints received. The number of complaints received to date are in the millions.
£ value saved	
Number of "bad actors" identified	As this is a live investigation identification of the 'bad actors' continues.
Qualitative impact	It is hoped that bad actors will be identified and enforcement action taken.