Which?

2 Marylebone Road
London NW1 4DF
020 7770 7000
which.co.uk

Home Office
2 Marsham Street
London
SW1P 4DF

Protecting consumers by preventing fraud: data-sharing measures

Supplementary evidence on data sharing to Which?'s recommendations for the next fraud strategy

Submission date: 19/12/2025

Summary

This document is an analysis of the Home Affairs Select Committee's unfinished 2023-24 inquiry into fraud and its impact on victims. According to the Chair of the committee, **"the irregularity in data sharing between industries is a key barrier to building a whole system, data-driven response to tackling fraud in the UK."** This is disappointing because our evidence shows that a significant majority of victims (75%) are comfortable with their data being shared across organisations to help prevent future scams; and six in ten (61%) consumers think it is important that businesses and governments share data with each other as a way to tackle fraud.

The publication of the inquiry's findings would have provided scrutiny of the government's previous fraud strategy, and would have provided a mechanism to hold government and other key actors accountable for further delivery in this space in the next (forthcoming) fraud strategy. But Parliament was dissolved in mid-2024 before the inquiry could report its findings. This submission is an attempt to address that gap in relation to the evidence about data sharing, ahead of the next government fraud strategy.

Only two major tech companies, two major telecoms companies, and three of the UK's top five banks gave evidence, suggesting a lack of engagement with parts of industry with the process. This is even more striking in the context of industry-led voluntary charters to prevent fraud, and which include commitments around data-sharing.

The evidence that was submitted shows a landscape of fragmented, relatively small scale data sharing initiatives. Stakeholders cited perceived legal barriers, technical barriers, commercial barriers and data quality issues, as reasons why they were not sharing more data. Although stakeholders made proposals for solutions to perceived legal and technical barriers, no solutions were proposed for perceived commercial barriers or data quality issues.

Which? believes that government mandated data sharing is necessary to ensure that all relevant stakeholders are participating in data sharing schemes to reduce fraud and its impact on victims. We also reiterate our call that the government lead by example by sharing its own data.

Introduction

In September 2023, the Home Affairs Select Committee launched an inquiry into fraud. The inquiry had a specific focus on the impact of fraud on victims, due to the devastating impact fraud has, both in terms of financial losses and "lasting mental health trauma." In 2023, the year in which the inquiry was launched, fraudsters stole approximately £1.17 billion from consumers according to UK Finance, a number which has remained broadly unchanged in subsequent years. Which? research has found that being a scam victim is associated with significantly lower levels of life satisfaction, lower levels of happiness and higher levels of anxiety. We estimate that this lower level of life satisfaction is equivalent to an average impact of £2,509 per victim, or £9.3 billion per year across all victims.

The committee was due to publish its report in autumn 2024 but the general election of July 2024 meant Parliament was dissolved before the inquiry's findings were published. Instead the Chair of the inquiry wrote a letter with a high-level outline of findings. This letter highlighted the importance of data-sharing, and that the evidence to the inquiry on this topic had surfaced inconsistent and sometimes limited data sharing between actors in the counter-fraud chain. This is disappointing because our evidence shows that a significant majority of victims (75%) are comfortable with their data being shared across organisations to help prevent future scams; and six in ten (61%) consumers think it is important that businesses and governments share data with each other as a way to tackle fraud. According to the committee, **"the irregularity in data sharing between industries is a key barrier to building a whole system, data-driven response to tackling fraud in the UK."**

The Home Office fraud strategy in place at the time of the inquiry was due to cover the period between May 2023 and December 2024. The publication of the inquiry's findings - which was expected to take place in late 2024 or early 2025 - would have provided scrutiny of the government's approach, and would have provided a mechanism to hold government and other key actors accountable for further delivery in this space. But as a result of the inquiry not publishing its findings, there is not a comprehensive, transparent picture of the fraud prevention landscape and the efficacy of government fraud strategy, and there is no mechanism to link the government's future fraud policy work to the body of evidence collected by the committee.

This submission is an attempt to correct that gap in relation to the evidence about data sharing to prevent fraud. We are focusing on data sharing because we agree with the inquiry's contention that the irregularity in data sharing between industries is a key barrier to building a whole system response to tackling fraud in the UK, and therefore to reducing the impact which fraud has on UK consumers.

Background: Which?'s policy work on data-sharing to prevent fraud

Our 2023 paper on data sharing to prevent fraud demonstrates how intelligence about fraudsters can help operators in the counter-fraud chain (such as telcos, platforms, banks and law enforcement bodies) understand the tactics and personas of the scammers who use legitimate business services to target consumers.

We argued that, in order to be truly successful, data sharing must be both cross-sector and public-private. However, stakeholder engagement carried out by Which? to inform the paper highlighted several barriers that make anti-fraud data sharing difficult for businesses. These barriers were: concerns around breaching data protection regulation; the legal, technical and administrative costs of participating in data sharing schemes; and competition concerns, including around the asymmetric benefits of data sharing.

In May 2025, Which? submitted a series of recommendations to the Home Office, detailing what should be included in the next fraud strategy to keep consumers safe from fraud. In that submission, we argued that data sharing can help businesses in the fraud ecosystem to build better anti-fraud systems. We called on the government to drive forward work to overcome these barriers and facilitate data sharing for fraud prevention, as well as to lead by example by sharing its own data.

Our approach to the inquiry evidence submissions

In order to understand the fraud data sharing landscape and to help inform the government's future policy work on fraud data sharing, Which? has reviewed all of the written and oral evidence submitted to the Home Affairs Select Committee's 2023-24 inquiry into fraud to assess what relevant stakeholders in the fraud prevention chain said about data sharing. We followed this up by engaging with several of the organisations who submitted evidence to the inquiry to ask further questions about data sharing. In particular, we sought to understand:

- which organisations did and did not provide evidence about data sharing;
- what data sharing is already taking place for fraud prevention;
- what data firms want access to for their fraud prevention efforts;
- what the perceived barriers are to data sharing; and
- what the perceived solutions are to overcome those barriers.

Which organisations did and did not provide evidence about data sharing

80 discrete actors - both organisations and individuals - submitted evidence to the inquiry in either written or oral form, and of these 45 mentioned data sharing in one respect or another. The level of engagement varied considerably across different sectors within the counter-fraud chain.

The telecoms sector had the lowest level of engagement with the inquiry. Out of the eight signatories to the 2022 Telecoms Fraud Charter (which promises, amongst other things, that telecoms providers will share information with other telecoms providers, banks and law enforcement to detect and reduce fraud), only two, BT and EE (owned by the same parent company and accounting for 23 million UK customers according to Signalchecker), submitted evidence to the inquiry. Other large telecoms firms such as VodafoneThree (28.8 million customers), Virgin Media O2 (15.6 million contract mobile customers), Tesco Mobile (5.7 million customers), Sky (3 million customers), and TalkTalk (now discontinued, but previously with around 3 million UK subscribers) did not submit any evidence. Given that, per the Payment Systems Regulator, approximately 26,580 APP fraud cases in 2023 (12% of the total) originated from telecoms companies, this low level of engagement from the telcos sector is very disappointing.

Levels of engagement within the tech sector were not much stronger. Only seven out of the thirteen tech sector signatories to the 2023 Online Fraud Charter submitted evidence to the inquiry, and six of those eight signatories are owned by three companies: Google (62.7 million UK users) and YouTube (55.5 million UK users) by Alphabet; Facebook (38.3 million UK users) and Instagram (37.3 million UK users) by Meta; and Microsoft (43.4 million UK users of LinkedIn and 3 million users of Bing). The other signatory who submitted evidence to the inquiry was techUK, the industry association. This leaves six independently owned tech sector entities which did not give evidence to the inquiry: Amazon (52.7 million UK users), Snap (23.9 million UK users), TikTok (23.3 million UK users), X (19 million UK users), Match Group (2.9 million UK users), and eBay (number of users not available). Meta and Google both discussed data sharing in their response, while Microsoft did not, despite the fact that the Online Fraud Charter commits signatories to engage with initiatives to quickly share information about frauds. Again, this level of engagement from the tech companies is disappointing, given that (per the Payment Systems Regulator) Facebook accounted for 90,827 APP scams (41% of the overall volume) in 2023, followed by Instagram (17,722; 8%), Snapchat (8,861; 4%), X (6,645; 3%) and Google Search (4,430; 2%).

Engagement with the subject of data sharing was also mixed within the financial services industry. Three of the UK's five largest banks by customer base engaged with the inquiry: Barclays (48 million customers), Lloyds (27 million customers) and Nationwide (16 million customers), as well as Santander, which is not in the top five. The UK's second and fourth largest banks in terms of customer numbers, HSBC (41 million) and NatWest (19 million), did not submit evidence to the inquiry. Various other financial services firms and trade associations, such as Mastercard and UK Finance, engaged with the inquiry. Financial services firms, including the aforementioned banks, Mastercard, TransUnion, and several trade associations (including UKFinance, Innovate Finance and Pay.UK) made up 13 of the 45 respondents who mentioned data sharing. This compares to three actors representing the tech sector (techUK, Meta, and Google) and just one representing the telcos (BT Group).

There were six submissions from law enforcement organisations regarding data-sharing; five from government bodies and regulators; five from non-profit organisations (including Cifas and Stop Scams UK); five from academics; one from the insurance industry; one from the digital advertising industry; and one each from LexisNexis Risk Solutions, PwC UK, Sainsbury's, the British Phonographic Industry, and a private individual. Striking gaps are the Information Commissioner's Office, the body responsible for overseeing rules around data sharing, and Ofcom, which has duties to enforce the Online Safety Act in relation to fraud, did not give evidence.

From reviewing the list of who submitted evidence to the inquiry, and which evidence submissions mentioned data-sharing, a striking picture emerges of particularly low engagement from telcos and tech companies despite commitments made in their respective voluntary sector charters; and particularly low engagement from the public sector.

What data sharing is already taking place?

The evidence submitted to the Home Affairs Select Committee's inquiry about data-sharing initiatives is fragmented.

Intra-sector data sharing - data sharing which happens between organisations in the same sector - is well-established, particularly in the financial services industry. Examples include Mastercard's Mule Insights Tactical Solution, a system which tracks the dispersion of illicit funds through the Faster Payments and Bacs systems and alerts participating financial institutions to suspected mule accounts; work being undertaken by Santander to develop an intra-bank data sharing initiative; and the Global Fraud Detection network operated by Pay.UK and Visa, which enables both companies to share information about fraudulent activities and trends with financial institutions and merchants worldwide.

There were examples of data sharing from the private sector to the public sector. Lloyds Banking Group said that it works with the City of London Police to support arrests and disrupt criminal gang activity. Vodafone Three told Which? that it currently shares data with law enforcement agencies upon any lawful request. Meta told the Select Committee that it proactively shares fraud reports with law enforcement. There was no evidence of data-sharing from the public sector to the private sector.

Several of those who gave evidence to the inquiry reported participating in cross-sector data sharing schemes. For example, Meta cited its participation in the Fraud Intelligence

Reciprocal Exchange (FIRE), an intelligence sharing pilot which it launched in October 2024 in collaboration with NatWest and Metro Bank. Santander cited its work as part of Stop Scams UK (a membership organisation of businesses from across the banking, technology and telecoms sectors which seeks to develop data sharing solutions) to share data to prevent fraud. Mobile network Three told Which? of its participation in Stop Scams UK's Project Trojan, an initiative to share data from the government's 7726 reporting service for fraudulent text messages. Stop Scams UK announced in October 2025 that every UK mobile network operator and 99.7% of UK retail banking providers were part of its membership, but the announcement notes that Virgin Media O2 and VodafoneThree had joined in recent weeks, suggesting that neither was a member at the time of the inquiry, and that neither were therefore participating in Stop Scams UK's data sharing initiatives at the time of the inquiry. The Global Signal Exchange, overseen by the Global Anti Scams Alliance, includes participants from a range of sectors, including online platforms and telecoms companies. Amazon, which did not submit evidence to the inquiry but which is a signatory to the 2023 Online Fraud Charter, is a participant in the Global Systems Exchange, alongside Google and Meta; but there was no evidence from the inquiry to suggest that Online Fraud Charter signatories X, TikTok, or Snap were participating in any form of data sharing.

As before, from reviewing evidence about current data-sharing initiatives to prevent fraud, what is most striking is the gaps. Numerous organisations with millions of customers who have signed industry charters which make explicit pledges in relation to data sharing to prevent fraud do not appear to be actively participating in data sharing initiatives. There also seem to be strategic gaps in public sector data-sharing.

What data firms want access to for their fraud prevention efforts?

Of those who did respond to the inquiry, only one stakeholder - Barclays Bank - outlined specifically to the inquiry what data they want access to in order to help prevent fraud. Barclays cited victim characteristics, transaction channel information, mule account details, and threat actor characteristics as key data points that would help organisations to prevent more fraud.

This data is a combination of sensitive and personal data on the one hand (victim characteristics, mule account details, threat actor characteristics), and operational data on the other (transaction channel information). The operational data points are less likely to include personal information and are therefore less legally complex than data points such as victim and threat actor characteristics and mule account details.

This is important to note because it demonstrates that, while it may be necessary to use sensitive data for certain kinds of fraud prevention, it is also possible to engage in counter fraud data sharing without using sensitive data. This means in turn that organisations in the fraud prevention chain cannot use legal complications as a blanket reason for not sharing data.

What are the perceived barriers to data sharing?

Respondents from all across the fraud ecosystem cited perceived legal barriers to effective counter fraud data sharing. UK Finance (the UK financial services trade body), for example, spoke about an absence of legal gateways to permit regulated firms to share information with each other without liability for breach of confidence. Barclays spoke about complex privacy and data sharing laws hampering fraud investigation and reporting across institutions. TechUK (the UK tech trade body) called on the government to establish legal mechanisms and pathways for lawful exchange of data, while Google also referred to legal challenges.

During the inquiry, the Economic Crime and Corporate Transparency Act (2023) removed the liability which financial services institutions might face when sharing data for the purposes of countering economic crime, which would seem to challenge the assertions made by Barclays and UK Finance. Furthermore, since the dissolution of the inquiry, in November 2024 the ICO, the UK's data protection regulator published guidance to clarify "data protection law does not prevent organisations from sharing personal information, if they do so in a responsible, fair and proportionate way". Most recently, the Data (Use and Access) Act (2025) has introduced the concept of 'recognised legitimate interest' as a ground for processing data, with the prevention of crime explicitly listed as an example of a recognised legitimate interest.

Some organisations cited technical barriers to data sharing. UK Finance said that no mechanism has been identified which will support the ingestion of relevant data from regulated sectors within a set service level agreement, and that current systems are not interoperable. Meta reported that it does not proactively share data with law enforcement because the scale of the data shared would be difficult to manage.

TechUK spoke of commercial barriers that prevent private companies from sharing information about their customers, while Which?'s own stakeholder engagement has highlighted the asymmetric benefits of participating in data sharing schemes as a major blocker to effective data sharing. Some stakeholders told Which? that data sharing schemes can enable firms with weaker fraud protections to benefit from the investment that other firms have made into sharing their data; in essence, they use insights from other organisations to improve their systems, rather than investing in doing so themselves. Stakeholders cited this as a reason for some firms' (i.e. those who would not be the beneficiary of the asymmetric benefits) reluctance to participate.

Some organisations cited issues of data quality as to why they are not sharing data. The Cybercrime and Online Harms Practitioner Network (COPRNET), a network bringing together law enforcement, researchers and other organisations, said in its evidence submission that under-reporting of fraud by victims remains a challenge, as it raises questions about data quality, among other things. This is supported by Which? research, which found that the two most common reasons victims did not report fraud were that they did not know that they could report fraud to a specific stakeholders - be they banks, the government, or the website/app hosting the scam - and that they did not know how to report fraud to that stakeholder. In contrast Meta argued that the usefulness of the data it could share with law enforcement would be limited and possibly unhelpful, because not all fraud reports from users were genuine - ie there is over-reporting of fraud. While we cannot speak to the accuracy of Meta's specific claim, it is worth noting that Ofcom's recent report - Online Safety in 2025 - found poor engagement from a small number of online providers with respect to providing routes for fraud reporting, and that "substantially more needs to be done by tech companies to address [fraud]." Given this, it seems unlikely that Meta's experience of over-reporting is typical of the tech sector in general.

These perceived legal, technical and competition barriers were also identified in our 2023 policy paper on data-sharing to prevent fraud, so it is clear that they must be a priority.

What were the proposed solutions?

In order to address the problem of legal barriers, some stakeholders suggested that the government use the law to make data sharing mandatory. For instance, Barclays said that policymakers should mandate that card networks share detailed fraud information, while Pay.UK, the organisation which runs the UK's retail payments operations, said to Which? that the government should support regulators to mandate a UK-wide data sharing agreement for Payment Service Providers.

Other stakeholders called on government to amend the legislative framework to enable more data sharing. For example, Lloyds recommended that the government extend provisions under the Economic Crime and Corporate Transparency Act to enable greater information sharing between banks, social media platforms, and telecoms companies; Stop Scams UK called on the government to remove the regulatory barriers to data sharing via reform of data protection law; and TechUK stressed the need to establish legal mechanisms and pathways for the lawful exchange of data. Finally, the Home Affairs Select Committee recommended in its letter to the Home Secretary that the government should consider introducing further legislation to extend the provisions under the Economic Crime and Corporate Transparency Act 2023 to enable information sharing between banks, technology, social media, and telecommunication companies, with measures that mandate information sharing for the purposes of tackling fraud. Cifas said that legislation must be backed by a long-term policy vision from the government.

On the subject of technical barriers, some stakeholders proposed technical solutions to enable more data sharing. Nationwide said that the government should explore a central hub which brings together industry, government, and law enforcement to share data to prevent fraud. The Payments Association, the trade association for the UK payments industry, said that there was a need to align data sharing requirements and infrastructure across various fraud mitigation initiatives which are already ongoing.

Meta said in its evidence submission that the government must use its power to convene to encourage more cross-industry collaboration, but it wasn't clear which specific barrier this could address.

None of the respondents explicitly proposed a solution to the commercial barriers or the issue of data quality.

Overall takeaways

The evidence provided to the Home Affairs Select Committee's inquiry suggests a lack of engagement with the issue of data sharing to prevent fraud amongst some large organisations in key sectors. These organisations will likely have useful information on scams which could, if shared, be used by other organisations in the fraud prevention chain to prevent scams, and so their lack of participation is likely reducing the overall potential effectiveness of data sharing for fraud prevention.

This was especially true in the telecoms space, where very few organisations responded to the inquiry at all; as well as the tech space, where response rates were higher but still comparatively low. Engagement within the financial services sector was stronger, though there were still some notable organisations which did not engage with the inquiry.

The inquiry did not shed much light on the kinds of data that needs to be shared to prevent fraud. But there was some indication of the usefulness of operational data, which is not a sensitive category of data.

The evidence of the data sharing which is already taking place suggests that the data sharing which is taking place is limited. While numerous organisations with large user/customer bases, such as Meta and Lloyd's Bank, did provide some evidence of their participation in data sharing schemes, numerous organisations with large user bases, such as X and Vodafone, did not provide any evidence of doing so.

The most commonly cited barrier to data sharing was legal, but the regulator has subsequently been clear that the law itself presents no such barrier. However, given the continued perception of legal issues, the suggestion that the ICO should issue new guidance on data sharing and fraud could be helpful in addressing those perceived issues.

Perceived technical barriers were also cited, and some solutions proposed such as a government-run central hub or repository for shared fraud data. Commercial barriers (including the issue of the asymmetric benefits of participating in data sharing schemes) and barriers around data quality were also raised with the inquiry, and no solutions proposed.

Next steps

In Which?'s view, mandatory data sharing is the only solution which will address the issues of perceived legal barriers, technical barriers and commercial barriers, and which the Home Affairs Select Committee's inquiry as well as our own stakeholder engagement have highlighted. The government is planning to relaunch its fraud reporting service in early 2026, a move which might address issues of data quality.

The lack of engagement by significant amounts of the fraud prevention chain with the inquiry, and the fact that many of the signatories to the voluntary sector charters have not provided any evidence of participating in data sharing schemes despite having explicitly agreed to do so in the charters, suggests to Which? that continuing with the voluntary approach would not be effective. **The voluntary approach has not incentivised these players to participate, meaning there is a case for the government to make their participation mandatory.**

Moreover, a mandatory approach would help to address the issue of asymmetric benefits to data sharing which our stakeholder engagement has highlighted previously, and for which no other actor is proposing solutions. Addressing concerns around data sharing regulation and any technical or quality barriers to data sharing is of course helpful, but if some companies continue to believe that their competitors might gain more than they do from participating in data sharing initiatives, they will remain unlikely to participate in those initiatives. The threat of legal action for non-participation can create the incentives for all companies to participate in data sharing initiatives.

A mandatory approach will incentivise firms to collaborate to overcome technical barriers to data sharing. Government can also - as was suggested in the inquiry - contribute by working with industry to build a technical solution, as has been the case in Australia.

Australia's Scams Prevention Framework provides an example of how a mandatory data sharing system can work in practice. The framework requires "regulated entities" (defined by the legislation) to share any "actionable intelligence" (i.e. data from scam reports) with the Australian Competition and Consumer Commission (ACCC), which can then disclose said information to other "regulated entities." This framework is underpinned by Australia's National Anti-Scams Centre (NASC), which receives scam reports from regulated entities and cascades them to relevant stakeholders.

The centre was initially operationalised without the underlying legislation in place, though it was clear from the beginning that legislation would be passed to create statutory duties in relation to data sharing in due course. Thus, while firms are currently sharing data 'voluntarily', they are doing so in the knowledge that will be obliged to do so from 1 July 2026.

In the first year of the NASC's operation (2024), reported losses from scams fell by 33% from the 2023 figure, while the number of reported scams fell by 17%, according to official government statistics. The statistics currently project a further decrease in both scam losses and scam volume during 2025. In terms of cost, the Australian Government's impact assessment for the policy suggests upfront data sharing costs of A$40,000 each (~£20,000) for major banks, A$250,000 each (~£125,000) for telcos, and A$1 million each (~£500,000) for major and medium sized online platforms, as well as respective ongoing annual costs of A$20,000 (~£10,000), A$70,000 (~£35,000) and A$300,000 (~£150,000). Given the huge costs that fraud imposes on the economy (£18.9 billion per year according to the Online Safety Act's impact assessment), such relatively modest investments (given the resources of those who would likely be in scope of such a policy) would be justified, in our view.

The government should use its forthcoming fraud strategy to outline a clear path towards mandatory data sharing initiatives, accompanied by clear timelines for the delivery of such initiatives, in order to ensure accountability. If it continues to rely on the voluntary approach it has pursued thus far, then cross-sector data sharing is likely to remain inconsistent and limited and, therefore, ineffective.

About Which?

Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent consumer voice that works with politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we're not for profit and all for making consumers more powerful.

For more information contact:
Matthew Niblett
Senior Policy Advisor
matt.niblett@which.co.uk
December 2025