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

Home Office
2 Marsham Street
London
SW1P 4DF
United Kingdom

Consultation Response

Which? response to the Home Office's consultation on economic crime information sharing

Submission date: 14/05/2026

Summary

Which? welcomes this opportunity to respond to the Home Office's consultation on economic crime information sharing. Fraud, a category of economic crime, is the UK's most widely-reported crime, with an estimated 4.4 million incidents in the year ending December 2025, according to the Crime Survey for England and Wales. This means that fraud accounts for approximately 46% of all crime in England and Wales. UK Finance estimates that, in 2024, consumers lost £1.17 billion to fraud. Fraud also causes major financial and psychological harm to consumers. The best way to mitigate this harm is to prevent fraud from happening in the first place. Information sharing between different parts of the private sector and between the private sector and the public sector is an important component of fraud prevention. However, information sharing is currently fragmented and inconsistent, due to perceived legal barriers, as well as technical barriers, commercial barriers, and issues of data quality. The best way to address these barriers is for the government to make participation in data sharing schemes mandatory. There are also a number of specific interventions which the government can make to address issues with data sharing, including expanding the scope of the Economic Crime and Corporate Transparency Act and being proactive in sharing its own data.

The main body of our response will focus on question 3.6, *How else could government better support private-private information sharing for economic crime purposes;* and question 9.2, *Please consider how else Government could better support information-sharing between public and private bodies for economic crime purposes*?

We have also provided answers to question 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;* and question 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?

Full response

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

Fraud is the UK's largest crime, with an estimated 4.4 million incidents in the year ending December 2025, according to the Crime Survey for England and Wales. This means that fraud accounts for approximately 46% of all crime in England and Wales. UK Finance estimates that, in 2024, consumers lost £1.17 billion to fraud.

The harm caused by fraud is not only financial, but also emotional and physical. Which? research estimates that the emotional damage associated with being a victim of fraud equates to £9 billion per year across the UK population. 9% of fraud victims polled by the Social Market Foundation reported an impact on their physical health as a result of fraud victimisation.

Fraud victimisation also has longer-term consequences. According to the Global Anti Scams Alliance State of Scams report for 2025, 30% of those who were scammed said they were more vigilant as a result, 17% said they were more distrustful of digital tools and platforms, and 14% reported a drop in their confidence. Which? research has found that 73% of consumers who had experienced scams changed their purchasing behaviour, choosing to shop with familiar companies as a consequence.

Which? has previously argued that the best way to reduce the myriad harms caused by fraud is to prevent fraud from happening in the first place. There are two key components to fraud prevention: individual sectors (online platforms, telecoms networks, payment service providers) adopting measures to make it more difficult for fraudsters to use their services to target consumers; and all sectors sharing information about fraudsters and their strategies with one another and with the public sector.

Which? is not the only organisation which has emphasised the centrality of information sharing to tackling fraud. The National Crime Agency told the Home Affairs Select Committee's fraud inquiry in 2024 that data and intelligence can be used to disrupt fraudsters before they act. The Home Office has stated that public-private and private cross-sector cooperation is critical to responding to fraud and that effective information sharing is the key enabler of that cooperation.

However, evidence from relevant stakeholders points to "highly inconsistent and sometimes limited data sharing between actors across the counter-fraud chain", according to the former Chair of the Home Affairs Select Committee. The committee, which ran an unfinished inquiry into fraud between 2023 and 2024, concluded on the basis of the

evidence it had received that “irregularity in data sharing between industries is a key barrier to building a whole system, data-driven approach.”

Which? analysis of the evidence submitted to the Home Affairs Select Committee, as well as stakeholder engagement conducted in 2023, points to several factors explaining the inconsistency of public-private and cross-sector data sharing in the UK. These were: perceived legal barriers; technical barriers; commercial barriers; and issues of data quality. We also found a lack of engagement with the question of data sharing among certain sectors, particularly telecoms and technology companies, as well as the public sector.

The lack of engagement by significant amounts of the fraud prevention chain with the previous Home Affairs Select Committee inquiry on fraud - only two of eight signatories to the Telecoms Fraud Charter and only seven of thirteen signatories to the Online Fraud Charter submitted evidence - suggests to Which? that continuing with the voluntary approach would not be effective. The voluntary approach has not incentivised enough players to participate in data sharing, meaning there is a case for the government to make participation mandatory. This is reinforced by the fact that Which? research shows that 61% of consumers think it is important that businesses and governments share data with each other as a way to tackle fraud.

Many stakeholders, including UK Finance and TechUK, have cited perceived legal barriers to data sharing, despite the fact that the ICO has published guidance which states that “data protection law does not prevent organisations from sharing personal information, if they do so in a responsible, fair and proportionate way.” In Which?’s view, mandatory data sharing is the only solution which will address these perceived legal barriers, since it will provide companies with a concrete incentive to share data. The Home Affairs Select Committee suggested that the government extend the provisions of the Economic Crime and Corporate Transparency Act 2023 which guarantee anti-money-laundering-regulated firms an exemption from civil liability for sharing information to prevent economic crime. Which? supports this proposal, as it might assuage some concerns among telecoms and technology companies that they could face civil liability actions for sharing information, something which the government has cited as a barrier in its call for evidence.

A mandatory approach will also incentivise firms to collaborate to overcome technical barriers to data sharing. Stakeholders including Nationwide and The Payments Association have suggested the creation of a central hub to address technical issues. The government’s Online Crime Centre has the potential to achieve this; the government must ensure that addressing technical challenges is a priority for the new centre. Government could, for example, develop the Online Crime Centre into something akin to Australia’s National Anti-Scam Centre. The centre - which cost A$58 (approximately £31 million) to build - receives scam reports from online platforms, telecoms operators and payment service providers and cascades them to relevant actors in the fraud chain, both in the private sector as well as regulatory and law enforcement bodies. 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.

A mandatory approach would help address the issue of asymmetric benefits to data sharing, something that was highlighted during Which? stakeholder engagement on the

subject of data sharing. Some businesses with whom Which? spoke were concerned that participating in data sharing schemes might help their competitors. They were worried that the data they shared could be used to harm their reputation or that their intellectual property could be used to train systems that are sold by their competitors for a profit. Addressing concerns around data sharing regulation and any technical or quality barriers to data sharing would be 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. The threat of legal action for non-participation can create the incentives for all companies to participate in data sharing initiatives.

The government's new fraud reporting tool - Report Fraud - could have the potential to address issues of data quality. However, Which? research found that only 19% of consumers used Report Fraud's predecessor, Action Fraud. The government must ensure greater uptake of Report Fraud by making it easy for consumers to access (for example, via integrations with online platforms). This is especially important, as our research found that, among those who did not report their fraud experience to Action Fraud, 24% did not do so because they did not know how. It must also ensure that Report Fraud data is being shared with the Online Crime Centre and relevant parties in the private sector. Again, our previous research found that one in five consumers who did not report scams to either their bank or to the platform hosting the scam did not do so because they did not know how.

As we have argued before, the government holds important data for establishing the identities of individuals and businesses, including data in HMRC and Companies House. By securely sharing this data with actors in the fraud ecosystem, it can help businesses to effectively filter out scammers misusing identities, thereby preventing fraud. In order for this to be effective, government must contribute its own data to the fraud prevention ecosystem to support businesses conducting due diligence checks to prevent fraudsters from reaching consumers.

9.3 Please describe your experience 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?

Members of the public can report malicious URLs through the Which? Scam Sharer tool. Which? owns this data, but shares malicious URLs with the National Cyber Security Centre on a weekly basis. Which? sends the URLs to Netcraft - the domain takedown service used by the NCSC. No personal details of the reportee are shared.

In order to fully comply with the Data Protection Act 2018 and UK GDPR, Which? and the NCSC signed a data agreement as well as a variation letter to allow Which? to share data directly with Netcraft and without the need for another agreement between Which? and Netcraft.

Only one designated email address can send the URL data that Which? shares. If any other email address attempted to submit the data, it would fail.

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 including any operational and legal considerations.

Smart Data

The Home Office, in this consultation, has defined Smart Data as a technology which can aid information sharing by tackling data fragmentation through common data formats, API-driven platforms, and risk-based sharing embedded with privacy-by-design. This, in the government's words, can create 'efficiency gains.' This framing does not grasp Smart Data's capabilities or use cases, nor does it capture the risks consumers could face in relation to fraud. We would like to see the government adopt a principles-based model for Smart Data trust frameworks in order to minimise the risks consumers could face.

The Department for Business and Trade's recent Smart Data Strategy states that 'Smart Data is about ensuring that individual consumers and businesses reap the benefits from their own data, in a safe, secure and interoperable system that also drives UK economic growth." Similarly, we have argued that the purpose of Smart Data is to 'give consumers the ability to share their data between businesses and other organisations, to enable new uses of data in ways that benefit consumers, society, and the economy.' Both Which? and DBT frame Smart Data as the interoperable, consent-based sharing of data for consumers' benefit. For example, schemes across multiple sectors can enable consumers to have greater choice in personalised services, leading to better prices and economic growth through services such as automatic switching or tailored account management. Smart data can also deliver 'efficiency gains' by enabling more secure data transfer between consumer businesses and third parties. However, we argue that, when seeking to optimise the gains of technologies such as Smart Data, the government must also be cognisant of the risks these technologies can pose.

We argued in our 2024 paper that consumers could face risks from Smart Data schemes if they are implemented poorly. For instance, consumers may be at increased risk of privacy loss and fraud if third parties are poor stewards of their data. Firms that meet data protection and sector regulatory requirements are still susceptible to data breaches or cyberattacks, and the greater the number of firms involved in handling consumer data, the more weak points will emerge where data privacy and security are compromised. In turn, we see data protection as necessary but not sufficient, and more direct actions are needed to make smart data secure beyond the current ICO guidance.

Vulnerable people are also at risk of exploitation if they are coerced into handing over highly personal and sensitive information, such as login details or if smart data is not fit for their needs. This could create a fertile environment for fraudsters to develop malicious apps that trick consumers. Our 2024 paper provides a principles-based model for trust frameworks that, when adopted, minimise the risks consumers could face. We would like to see this adopted across government to ensure the safe development of smart data.

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

May 2026