Which?

Sharing data to tackle fraud

POLICY PAPER | NOVEMBER 2023

Summary and recommendations

Fraud is a blight on the UK. It inflicts serious financial and emotional harm on millions of people across the UK every year. This is often orchestrated by sophisticated organised criminal groups who trade intelligence on the best way to target consumers. Currently business and government operate in silos and do not share the data they have on how these scammers operate. As a result efforts to prevent fraud are operating at a disadvantage. Sharing fraud intelligence allows for the better protection of victims against repeat victimisation; supports businesses to build better anti-fraud systems; and helps law enforcement track down the criminals perpetuating this harm.

Which?'s extensive engagement with businesses across key industries has highlighted three key barriers that make data sharing particularly difficult for businesses. These are:

1. **Data protection** – Businesses are concerned that sharing fraud intelligence increases the legal risk they face from data protection legislation. Although there are a number of measures in data protection legislation to facilitate data sharing to prevent fraud, guidance is not clear enough to ease business concerns.
2. **Cost** – Businesses face a range of legal, technical and administrative costs to participating in data sharing schemes. While participation can result in a substantial decrease in fraud, not all businesses have sufficient financial incentives to decrease fraud on their services.
3. **Competition** – Businesses are concerned that participating in data sharing schemes may help their competitors. They are worried that the data they share 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.

These barriers are each surmountable with leadership from central government. The Government must:

1. **Establish duties to prevent fraud in key sectors** – The Government must ensure that businesses in key sectors either see financial repercussions from fraud on their services (such as the banking sector) or have a duty to prevent fraud on their services (such as in the Online Safety Act). This will ensure that businesses are incentivised to tackle fraud and be willing to pay the **cost** of investing in data sharing schemes.
2. **Increase legal certainty** – The Government must work with the Information Commissioner's Office (ICO) to create new guidance that provides additional clarity on when and how businesses can share data to prevent fraud while still complying with **data protection** legislation.
3. **Set standards to facilitate data sharing hubs** – The Government must support the development of the data sharing ecosystem by setting the standards for how businesses should collaborate to share data. By working with industry the Government can help develop technical frameworks that address the **competition** concerns of businesses through measures like anonymisation and limiting queries to binary yes/no questions.
4. **Open Government data** – The Government must contribute its own data to the fraud prevention data sharing ecosystem. It holds a variety of data that is useful in verifying

the identity of businesses and individuals. By securely sharing this data with key businesses the Government can support due diligence checks to prevent fraudsters reaching consumers.

The scale of the fraud problem

Fraud is the most prevalent form of crime in England and Wales, resulting in huge losses to individuals and the wider economy. Fraud represents over 40% of all offences in England and Wales. In 2021 individual victims' lost £2.35bn to fraud.

The financial sums lost are not the full cost. Being a victim of fraud can have a serious impact on victims' emotional, psychological and even physical health. Our investigations team has heard countless experiences of people who've lost confidence in themselves, their ability to trust others and even requiring medical care to cope. Which? research released in 2021 calculated the annual cost to wellbeing associated with being scammed at £9.3bn, equivalent to a loss of £2,509 per year for every individual victim. This is far above the estimated average financial sum lost, which stood at around £600.

Which? has decades of experience in helping UK consumers impacted by fraud. Our helpline and investigations teams have helped individual victims and raised awareness of the different types of scams that harm consumers including through our scam alert service. This has informed our policy work to advocate for effective change to protect consumers from fraud, including incorporating fraud and fraudulent advertising in the Online Safety Act and duties to reimburse victims of scams within the Financial Services and Markets Act 2023.

Which?'s engagement with businesses across a variety of sectors, law enforcement, regulators, Government and the third sector has led to a specific focus on the importance of fraud data sharing in this effort.

The case for data sharing

The idea of cooperating to tackle fraud is not new. Cifas, a not-for-profit fraud prevention organisation has been operating since 1988, encouraging cooperation, mainly in the financial sector. However, in that time fraud has massively increased in scale and changed from a primarily analogue crime to a digital one. There is now a growing consensus that data sharing will be crucial to tackling fraud. Last year, the House of Lords Fraud Act 2006 and Digital Fraud Committee concluded that data sharing " is a critical component of the counter-fraud effort and must proactively be encouraged by regulators and legislation." In the UK Government fraud strategy it identified improving data sharing as a key cross-cutting theme in its anti-fraud work.

Which?'s research shows that large scale fraud is often undertaken by organised crime groups that operate across different digital services. Criminal fraud networks cooperate through complex communities trading expertise to better defraud consumers. When victims are scammed it is rarely confined to a single service. Fraudsters lead their victims from one digital channel to another until they reach their ultimate goal of a payment.

Each service that consumers use whether that is a bank, a telecommunications provider or an online platform sees only one part of the fraud journey. The cross-platform nature of fraud has caused increased interest from businesses and policy makers in data sharing. Sharing intelligence about bad actors and their tactics helps provide a more holistic picture of fraud and enables businesses to better disrupt fraudsters and to protect consumers.

Data sharing helps protect consumers from fraud in three ways:

1. **Better protection for victims:** Sharing data about the victims of scams can be useful to stop that person from being a future victim of a scam. Where a person's identity has been stolen by a scammer, sharing information about that identity can help services prevent the scammer from setting up further accounts in that person's name. Sharing data about victims can also help services identify people who may be vulnerable in the future to further scams
2. **Better understanding of fraudsters:** Better intelligence will allow digital service providers to better understand the tactics and personas of scammers that operate using their services. This intelligence should include the types of accounts, behaviours and content that are associated with scams. As a result, services will be enabled to build more effective systems, that continuously improve over time, to detect the scammers attempting to use their service and speed up take down in the event of a breach.
3. **Better intelligence for law enforcement:** Shared fraud intelligence can support law enforcement in tracking scammers across services and help to identify and take action against the organised crime that perpetuates these scams.

By failing to share effective intelligence, the anti-fraud ecosystem is putting itself at a disadvantage against fraudsters who actively cooperate to undermine these systems. Scammers operate in sophisticated networks that will share any exploit found that allows them to reach consumers. If data is not shared then businesses will continue to be one step behind the fraudsters. Services attempting to operate in silos will be unable to detect the patterns used by fraudsters and will be less effective at stopping fraud as a result.

The Barriers

We have engaged with a wide variety of businesses from across key sectors, for the last year, and they have made clear to us that they face three primary barriers which can make data sharing difficult. These are data protection regulation, costs and competition concerns. Our discussions have also highlighted that these can be overcome through central government leadership, clarity and action.

Data Protection

One of the most commonly articulated barriers are concerns that sharing fraud intelligence may breach data protection regulations. Organisations are cognisant that taking part in data sharing increases their legal risk. This is due to the nature of the General Data Protection Regulation (GDPR), including in its application in the UK. The GDPR is a principle based regime that sets out the principles that must be considered when processing personal data.

A key principle is that when processing personal data there must be a lawful basis. In terms of data sharing that means having a legitimate interest and conducting a balancing test to weigh that interest against the interests and rights of the data subject. This principle based approach means that there is regulatory risk to any activity involving data and organisations have invested heavily in data protection resources and policy processes as a result.

Which?'s legal analysis of current legislation and guidance finds that data protection law is constructed to support data sharing for the prevention of fraud. The GDPR recognises that preventing fraud is a legitimate interest. The ICO includes the example of a bank disclosing personal data about its employees to an anti-fraud body as an example of data sharing in their guidance.

In addition to requiring a lawful basis, data protection law requires the sharing of data relating to criminal offences to be for one of a list of specified purposes. These purposes include preventing or detecting unlawful acts, protecting the public against dishonesty and preventing fraud.

Many data sharing schemes do take advantage of the provisions in data protection law that facilitate sharing to prevent fraud. For example, Cifas publicly display their legitimate interest assessment for the National Fraud Database. This shows a way in which a data sharing scheme can pass the balancing test and meet data protection requirements.

The currently progressing Data Protection and Digital Information (DPDI) Bill proposes simplifying the requirements for processing data further. It will introduce the concept of a recognised legitimate interest where data processors will not have to undertake a balancing test. The Bill includes the prevention of crime as one such legitimate interest.

However, due to the principles based structure of data protection law there is still some legal risk that can make companies hesitant to share data. The organisations that have participated in data sharing to prevent fraud have been those which have a more sophisticated understanding of risk. These organisations have legal departments which understand the risk involved and how to effectively manage that risk.

Breaking the barrier

There is a clear opportunity to further lower that risk if the Government provides increased legal certainty. The ICO should use the opportunity of the changes in the new DPDI Bill to develop a code of practice containing practical, clear guidance in relation to sharing personal data for the purposes of detection, investigation and prevention of fraud. This will help more risk averse businesses to know how and when they can share data.

Alongside this industry can work with the ICO to gain greater certainty on the law in this area. Individual sector bodies should look to create codes of conduct on data sharing using Article 40 of the GDPR, which the ICO would be able to certify. Businesses with specific questions on how to interpret data protection law should make use of the ICO's innovation advice service which can help them in the development of data sharing schemes.

Cost

There are significant costs to setting up and participating in data sharing schemes and not every organisation has sufficient incentive to take part. These include:

- **Legal costs** to ensure compliance with data protection legislation (see previous section).
- **Technical and operational costs** to develop the systems through which to share data and to build interlinkages with existing systems.
- **Administrative costs** to develop the business case and to document and oversee the development of the data sharing project.
- **Membership or data acquisition costs** to join existing groups or to bring in external data in addition to the data sharing scheme.

Data sharing schemes create a benefit for participating businesses by helping them reduce the amount of fraud on their service. Interviews with data sharing service providers have suggested that billions of pounds in fraud loss has been prevented through data sharing schemes. For businesses that see a direct financial loss from fraud operating on their service this acts as a strong incentive to participate. This can be seen most clearly in the financial sector which is often on the hook for fraud costs and has the highest levels of participation in data sharing schemes compared to other sectors. As mandatory reimbursement is introduced by the Payment Systems Regulator (PSR) we expect this activity to increase, with banks proposing additional data sharing schemes to prevent fraud.

However, not all relevant businesses see a direct benefit from the reduction of fraud on their service. These businesses do not suffer a direct financial loss from fraud and see minimal consumers switching to services with less fraud. In addition, fraudsters are paying to use the service and so more effective fraud prevention would remove the fraudsters as customers and potentially lower revenue (although this is unlikely to be a substantial effect). In these cases Government intervention is necessary to create an incentive to partake in these schemes.

Breaking the barrier

The Government should ensure that key sectors are regulated and have duties to prevent fraud from operating on their service. This is the approach taken in the Online Safety Act. The Online Safety Act includes duties for user to user services to have proportionate systems to prevent users from encountering fraudulent user generated content and fraudulent advertising. Ofcom's codes of practice and guidance to implement the Act should include that platforms can use existing cross-sector data sources to determine if content is fraudulent and that data sharing will be key in establishing effective due diligence to prevent the placement of fraudulent advertising.

The telecoms sector is regulated by Ofcom but does not have the same clear duties to have proportionate systems to prevent fraud on their services. Other online sectors like emails and domains are not directly regulated. The Government should be actively engaging with participants in these sectors to encourage data sharing and should explore a possible need for future regulation to align the incentives of industry with the level of harm consumers face through fraud. The lack of action to share data in these industries aligns with their lack of incentive to tackle fraud compared to the financial sector.

Competition

It is not surprising that proposals for businesses to share key information with their competitors would cause concern. Our engagement has revealed mistrust and real fear that competitors could use incidence of fraud discovered on a service against each other to cause reputational damage. Businesses have the legitimate concerns that they could be granting an advantage to their competitors.

There is a cost to sharing fraud intelligence, so it reflects a businesses investment into their own fraud detection schemes. Once shared, all participants in the data sharing scheme benefit from that investment and this could mean that some benefit more than others. Some stakeholders engaging with Which? were particularly keen to note that smaller organisations who either have less fraud or weaker fraud protection will benefit disproportionately from larger firms' investment. Other stakeholders made the countervailing point that smaller organisations lack the capacity to fully participate in schemes and to take advantage of the intelligence gained from schemes.

A further concern was that the data gained through the data sharing scheme could be used to build more capable systems and those systems could then be sold to others. These fears were not evidenced but were repeated frequently by stakeholders across sectors.

Breaking the barrier

These concerns can be addressed through the choices made in the design of the data sharing scheme that will effectively mitigate them. Data sharing schemes can anonymise data sources so that any party using that data would not know which organisation it originates from. This could tackle concerns that shared data will be used to damage a business's reputation.

It is also possible to have more restrictive terms for how data from a hub can be used to prevent the sale of technology trained using data from that hub. For example, a scheme can restrict the response to data queries to a binary yes or no. This could help assure businesses that are concerned that their source data will be used to train a competitor's system that they could sell to others.

The Government has a role to bring key sectors and organisations together to discuss the structures that are needed to facilitate data sharing. The Government should ensure that appropriate models are available to counter the concerns of potential participants in these sectors. There is a need for central leadership to see swift progress across the sectors.

Effective structures for data sharing

Effectively structured data sharing schemes are key to overcoming the barriers that businesses face which can prevent them from sharing data. Data sharing schemes can either be bi-lateral, with two organisations collaborating, or hub based, which encourages the collaboration of many different players through data sharing hubs. Hubs can be focused on a specific sector or work across multiple sectors see diagram below.

There are two models of hubs:

- A complex shared database for pooling the data submitted by the different constituent members into one place. (Diagram A)
- A federated model for data requests where members hold their own data and the hub works as an intermediary to allow for checks to be run across the different data sets. (Diagram B)

Diagram A – Shared database

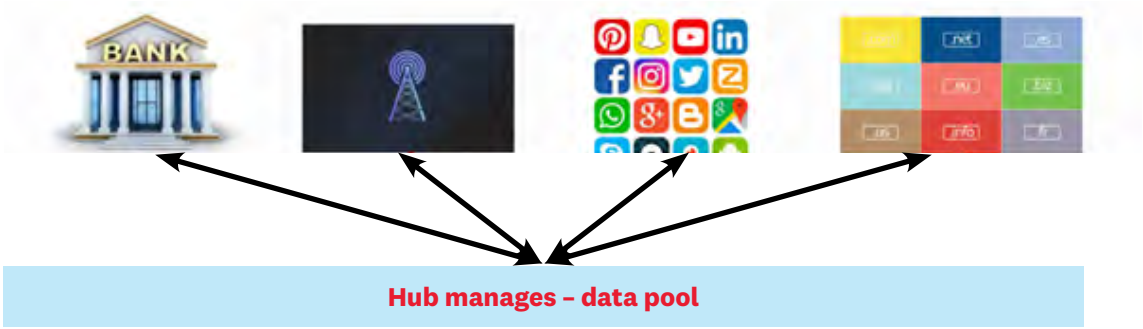
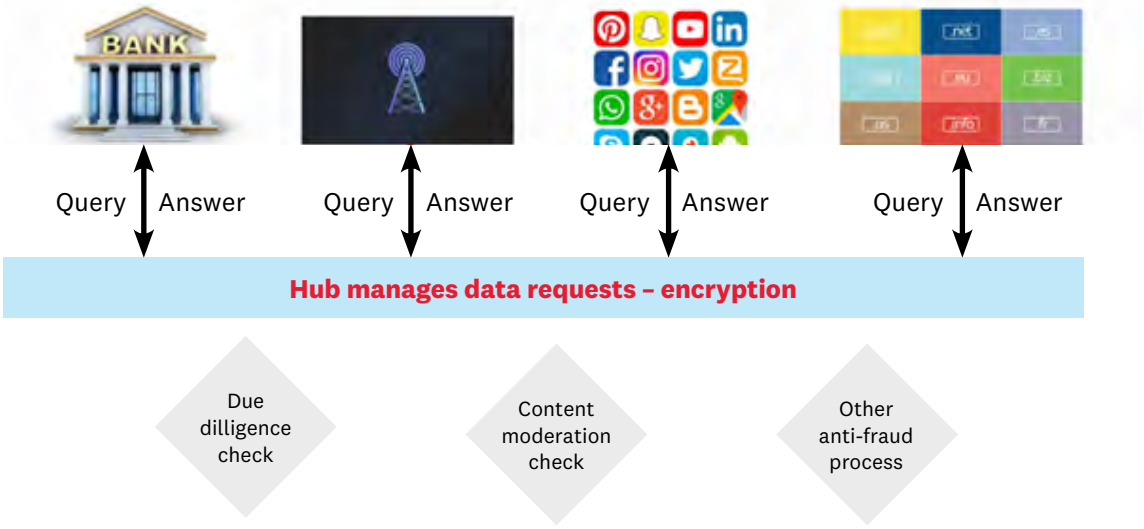


Diagram B – Federate Data model



Effective hubs have a variety of businesses contributing data and consuming data from the hub. The hub structure also allows for some businesses, where relevant, to consume data without inputting.

Hubs should play a key role in overcoming the barriers to data sharing by helping businesses with **data protection** compliance, provide a better **return on investment** by sharing data from more services, and their structure can mitigate **competition** concerns.

This compares favourably to bi-lateral data sharing which can require businesses to create bespoke business cases, data protection assessments and technical infrastructure for each new bi-lateral arrangement. By its nature bi-lateral sharing involves less data per-scheme as it only includes the two participants and so lacks the benefits of scale. Bi-lateral schemes

require trust between the two participants and cannot mitigate competition concerns. However, bi-lateral schemes can be useful where a tailored and easily adaptable approach is needed, particularly to support rapidly changing data sharing.

Our engagement with organisations already participating in various hub models found particular value in the benefits of combining data from a variety of sources. Deconfliction and trend analysis were seen as high value. In addition to the benefits of the technical structure of hubs, some of the most important benefits highlighted to us were from the human expertise located within hubs. This includes shared legal and business case templates and opportunities to informally share knowledge and techniques. It is also important to note that hubs and the community that builds around them can actively help facilitate the occasional need for bilateral data sharing where appropriate.

The Government's fraud sector charters could provide an invaluable spring board for sharing fraud intelligence if they recognise the importance of hubs as intermediaries. This requires central leadership and the Government should not hesitate to realise this opportunity.

Initial steps should include the government facilitating the development of the standards that underpin hubs. These necessary rules and requirements of participation in a hub are also known as a trust framework. This includes the assurance of the quality of data, the legal framework, and how the data will be used. Trust frameworks would aim to build assurance for all participants that their legal risk, cost, reputation and intellectual property concerns are mitigated. Examples of this in practice include the Government's digital identity trust framework and the UK Open Banking trust framework.

Building confidence and scaling up

Different industries are at different stages in their development of data sharing systems. While the finance and banking sector has a number of data sharing schemes to help them combat fraud other sectors, like online platforms, are less developed.

There are good reasons why it can be harder to develop data sharing schemes between online platforms. The construction of in depth data sharing within a sector revolves around the systems and protocols shared across that sector. The telecommunications, banking, email and domains sectors are all based on interconnected systems using shared protocols to establish cross-provider networks with similar functionalities that can be abused by scammers. For example, banks use the Faster Payment System to transfer money and domain providers use the Domain Name System (DNS). Data sharing within these sectors can be built to detect signals in these shared networks. The group of businesses that we refer to as online platforms offer a wide variety of services including online marketplaces, messaging services, social media and search engines. Aside from a few exceptions, such as the ActivityPub protocol which powers decentralised social networks like Mastodon, these are not based on interoperable systems and do not share common protocols.

Data sharing for online platforms will require the mapping of key data that can be usefully shared to help detect and prevent fraud. This can be solved gradually by putting in place easier to set up data sharing schemes as deeper data sharing is developed.

In the first instance organisations should be consuming all reasonably available data to establish that the user has a genuine identity and is not associated with fraud. This can be done in advance of setting up more developed data sharing schemes. Many platforms are already taking part in the Advertising Standards Authority (ASA)'s scam ad alert system where data is shared on the content of scam adverts and the URLs linked to within them. As announced in the Government's Fraud Strategy the National Cyber Security Centre (NCSC)'s share and defend programme that shares malicious domains will expand to technology companies in 2024.

We note that there is currently available data that consists of non-personal data that can be used by services to prevent fraud. This will allow data protection concerns to be addressed further down the line. Alongside sharing high-level expertise and trends on scams examples of non-personal data that can be usefully shared include:

- **Scam content** – The content of many public scam messages, posts or adverts can be shared either as is or in hashed form
- **URLs and Domains** – The full address of pages connected to fraudulent websites and associated domains.
- **Brand Identity** – The genuine details of brands including the social media accounts, URLs or contact details associated with known brands.

Alongside the use of non-personal data, these examples also show how organisations can, and do, safely share non-personal data into an appropriate hub.

There are more complex examples in other areas that have shown that organisations can use shared personal data to meaningfully tackle the harm that users face. Whilst banks are leading the way in fraud, in other areas platforms have proven they can progress with their shared databases that have been been established to combat Child Sexual Abuse Material (CSAM) thorugh the National Centre for Missing and Exploited Children (NCMEC) and terrorism through the Global Internet Forum to Counter Teorrism (GIFCT). These were created through effective pressure and collaboration from governments and civil society. There is not a direct analogue in fraud to the hashed images databases used in these cases. More work is needed to map the datasets that platforms hold in order to create shared databases of fraud behaviours and personas. Achieving this will require collaboration between platforms, the relevant government departments, Ofcom as the new online safety regulator, and civil society.

There is data held by the Government that could prevent fraudsters misusing individual and business identities. The Financial Conduct Authority's (FCA's) data has proven valuable to platforms in preventing fraudulent advertising. The Government should work through their fraud sector charters with other interested parties to understand what additional government held data could be used to support the development of fraud prevention tools. This could include data from HM Revenue and Customs (HMRC), the ICO, Companies House, and other sources that could be used to validate identity data.

The role of the Government

The Government has an important role in supporting the creation of a data sharing ecosystem to better prevent fraud. This includes:

- **Duties to prevent fraud in key sectors**
- **Increase legal certainty**
- **Set standards to facilitate hubs**
- **Opening government data**

Duties to prevent fraud in key sectors

The Government must ensure that sectors are either incentivised to prevent fraud by being directly financially liable for the costs of fraud or face regulation with substantial financial penalties if they fail to have proportionate systems in place to prevent fraud.

Increase legal certainty

The Government has a key role in overcoming business concerns on data protection. It must work with the ICO to ensure guidance on data sharing to prevent fraud is clear on how and when services can legally share data.

Set standards to facilitate hubs

The Government should facilitate the development of hubs by helping set standards to address business concerns through the development of trust frameworks. By working with industry the Government can ensure that trust frameworks are created that ease their concerns.

The Government should also work with the ICO on guidance to set standards for how data sharing schemes address people's right to rectification under data protection law. This would enable people who are incorrectly labelled as scammers to be able to set that right. Schemes should have systems that reduce the number of these 'false positives' and where they are informed of them take quick action to protect falsely labelled consumers.

Open up Government data

The Government holds important data for establishing the identities of individuals and businesses. This includes data in HMRC, Companies House and regulators. The Government must securely share this data into the fraud prevention ecosystem to help businesses effectively filter out scammers misusing identities.

Initial next steps – the next six months

The Online Fraud Charter in development between the sector and the platforms should be a catalyst for effective collaboration in this space. There has been effective public private collaboration pushing for better standards in cross sector groups, such as the Online Fraud Group. Initially, the Charter should be used to secure commitments to consume non-personal data including fraudulent domains and URLs. It should also begin explorative work to map relevant data sets and determine the opportunities for deeper data sharing between platforms.

Other sectors are similarly developing data sharing capacities to help tackle fraud. In the domains sector new tools have been developed to share data held by different organisations, such as those provided by the DNS Research Foundation, and improve reporting processes by the DNS Abuse Institute. Wider usage of these tools and greater collaboration in threat sharing should be a key focus of government engagement with that sector.

As it begins to implement the Online Safety Act, Ofcom should look to include requirements to consume data as it develops its initial codes of practice on illegal harms and related guidance. This should be followed with more extensive use of shared data as part of due diligence processes to prevent fraudulent advertising.

The Government should bring the DPDI Bill through Parliament to introduce the prevention of crime as a recognised legitimate interest for processing personal data. This will allow the ICO to begin work on updating the code of practice on data sharing for the prevention of fraud.

Which? believes that data sharing offers a huge opportunity to better protect consumers from fraud. We look forward to continuing to work with the Government and regulators as they develop and implement these schemes. They must be designed in a way to successfully help to overcome the harms currently faced by consumers as a result of the significant levels of fraud experienced in the UK.

Which?, 2 Marylebone Road, London NW1 4DF
Which?, 3 Capital Quarter, Tyndall Street, Cardiff CF10 4BZ
Phone +44 (0)20 7770 7000 Fax +44 (0)20 7770 7600 www.which.co.uk