INSTITUTE FOR GOVERNMENT

SCOTT LOGIC

ALTOGETHER SMARTER

DATA SHARING DURING CORONAVIRUS

Data sharing for counter fraud activities

Summary of a private roundtable

Paul Shepley and Gavin Freeguard

Introduction

This short report summarises a roundtable discussion held in summer 2022 looking at data sharing for counter fraud activities, including initiatives during the Covid-19 pandemic. It brought together academics, public servants from Cabinet Office and the British Business Bank and private organisations such as high street banks and identity verification services to discuss how data is shared between organisations and government to identify and prevent fraud. It draws mainly on discussions which took place at the roundtable. The roundtable was held under the Chatham House Rule – nothing anyone said is attributed to them or their organisation, unless they have asked for it to be. The discussion does not represent the views of the Institute for Government.

The roundtable forms part of a wider piece of Institute for Government research looking at government data sharing during the pandemic. The project takes six case study areas and uses a roundtable on each to explore what worked well, what could have worked better and what lessons government should learn for the future. Reports on each of the roundtables will be followed by a short synthesis report bringing together common themes in 2023.

Overview of data sharing for counter fraud activities

Data is a key aspect of any counter fraud activity, requiring a combination of personal and transactional data to be shared, often across multiple organisations including government and private sector organisations. While there were high-profile cases of government data sharing during the pandemic for counter fraud activities, such as with high street banks for the Bounce Back Loan scheme and other elements of business support, the increase in online activities necessitated by the pandemic increased opportunities for other types of fraud, such as identity fraud.

The roundtable discussion centred on activities around the Bounce Back Loan scheme during the pandemic. The scheme was established rapidly to provide urgent and immediate direct financial support to businesses who could request a loan of up to £50,000 from a high street bank, which were 100% guaranteed by the government. Ministers took the decision to launch the service quickly to save jobs and businesses from collapse, but in doing so accepted the risk of fraud in the scheme – now estimated by the business department as £4.9bn of fraudulent loans on a total of £47bn lent during the scheme.[1] The British Business Bank (hereafter the Bank), which was responsible for setting up the scheme, submitted both a reservation notice to the department and a request for ministerial direction* to proceed with the scheme, which outlined how the proposed scheme did not have a robust value for money assessment and presented a "very high" risk of fraud and error.[2]

To administer the scheme, the Bank had to collate and assemble data on which businesses were accessing the scheme (including name, address, contact information, loan value) from multiple lenders. Analysis then had to be presented in various formats depending on who was being reported to, including different ministers and departments. But there was not a large team of fraud or financial crime data experts at the heart of the operation identifying actual and potential fraud cases, and it has taken time to bring the right skills into the Bank. One participant explained how the lack of fraud expertise made it difficult to request the right data from lenders and set up the necessary data exchanges needed to identify fraud cases.

* A ministerial direction is a formal instruction from a minister to tell their department to proceed with a spending proposal despite an objection from their permanent secretary.

Key themes from the discussion

- Counter fraud schemes have historically required very specific data sharing agreements and the goodwill of participating organisations. Agreements were often motivated out of a joint desire to minimise fraudulent activity and business losses due to fraud.
- Data sharing for counter fraud, even with the Digital Economy Act 2017, is challenging due to the personal and identifiable data required to identify fraud. Challenges arise from the data being commercially valuable, held in different secure environments, being a mixture of commercial and personal data and more. Overcoming these challenges, especially in new schemes, requires time to establish data sharing routes – time which was often unavailable during the pandemic.
- There are numerous counter fraud data sharing initiatives ongoing, reliant on government and private sector collaboration.
- Participants agreed that in addition to technical challenges for data sharing, there is a cultural barrier to data sharing that must also be overcome.
- Future improvements could come from government collaborating with commercial financial organisations to establish a strategic data sharing framework, with pre-agreed standards on data format, security and an approach to regulation that facilitates information sharing whilst maintaining safeguarding standards. This would be especially useful during emergency situations, like the pandemic, by making it quicker to establish new data sharing agreements for novel purposes.

Counter fraud data sharing: a brief history

In terms of establishing data sharing agreements for any counter fraud activity, participants agreed the Digital Economy Act 2017 was a critical enabler. Before the Act, establishing a data sharing agreement that required legislation would take between 6 months to 2.5 years, depending on the legislative programme at the time. After the Act, civil servants were able to make decisions on data sharing agreements without recourse to legislation, making it quicker to reach agreement, often doing so within four weeks.

This speed was essential for data sharing during the pandemic and providing flexible agreements. Organisations could respond actively to threats of fraud or cyber attack that were visible in internal data by establishing data shares that could challenge the threats. If the threat then changed, the agreement could be quickly updated in response and new data could be added to the share to strengthen the response. This was necessary when administering Covid schemes and responding to fraud threats as they occurred.

Culture and skills continue to limit data sharing

One participant described that while there have been massive improvements in data sharing since the 2017 Act, and that this underpinned the government response to Covid overall, differences remain in the cultural attitude towards data sharing from different government departments. Some appear more concerned than others about data sharing, due to concerns about being exposed to problems, either from the legality of the data sharing or the nature of the information being shared. For example, this has limited the data and quality of data available to non-government analysts on Covid business loans. Limited access restricted the amount of analysis possible and therefore the ability to gain understanding from the data that has been collected and stored in the system.

An additional challenge mentioned by participants was the availability of counter fraud skills within the civil service. As the pandemic introduced new opportunities for cyber threats and fraudulent activity, "government, on some occasions, was having to set the rules at the same time as needing them to already be in place" reported Jessica McEvoy, formerly deputy director at the Government Digital Service (GDS) and now a principal consultant at Scott Logic. In some cases "government was able to rely on existing expertise, as well as reusing well-tested, well-built and well-thought-out platform technologies which helped to minimise the risk of fraud due to the long-term strategic view that GDS and the Digital, Data and Technology profession had taken take over the previous decade".

This was demonstrated in the resilience of the Universal Credit service, which relied on its existing infrastructure, albeit with some changes to enable faster payments during the pandemic. This was helped by the ready availability of counter fraud skills within DWP (which, with HMRC house the majority of counter fraud professionals in the civil service). Other departments were less able to respond, due to the poor distributions of relevant expertise.

For the Covid loan schemes, the lack of counter fraud skills in BEIS, the Bank or UK Finance, and the speed at which the scheme was established, led to increased levels of fraud in the early iteration of the system, which was a risk raised in the reservation notice and accepted by ministers. For example, it took almost a month to agree and establish a method for checking duplicate applications, during which 2.3% of approved applications were duplicates.[3] However, the lack of fraud and error expertise made establishing the right data sharing with private banks more difficult, as civil servants at the Bank were unsure of what data needed to be shared and had no experience in establishing the counter fraud data sharing agreements needed to share data across organisations and the financial sector.

Data sharing governance

For data sharing governance, participants discussed alternative ways to assess a data sharing agreement. This requires understanding the return on investment from sharing the data, in terms of both the resource required to support the data sharing and the risk taken on by agreeing to the data sharing. The risk element is particularly sensitive when identifiable data is being handled, including individual transactions. Protection of this data is improving, so that analytics can be conducted without knowing identifiable information, and then identity can be established only in specific cases where necessary.

When countering fraud of financial schemes, such as the Covid loan schemes, one participant described how in their view prevention of any payment is better than having to recoup an erroneous payment. This presented a particular challenge across the different business support schemes, including Bounce Back Loans. Fraud detection in this space would have required rapid data sharing during the application stage prior to any payment and this was lacking, in part due to there being various schemes (e.g. Coronavirus Business Interruption Loan scheme or CBILS, the Coronavirus Large Business Interruption Loan scheme or CBLBILS, and the Bounce Back Loan scheme) that were run independently from each other. This limited the amount of information available to share, or even a complete picture of what was going on across all the schemes in one place, leaving government unaware of the scale of fraud committed through the business support schemes and therefore how much resource should be used to conduct recovery activities.

Bounce Back Loan scheme

Considering the Bounce Back Loan schemes, the data required to check for fraud was held by private organisations in a combination of commercial and consumer datasets. This presented a challenge to sharing the data onwards into a secure central repository, administered by government, for analysts to assess. Due to this being a new requirement, the Bank had to work with the lenders to establish new data sharing agreements which allowed them to collate the loan and application details from all lenders, that could then be accessed by lenders (as noted for instance to check for duplicate loan applications). This was only achieved around a month after lenders started providing loans through the scheme.

One participant described the challenge of identifying duplicate loan applications. To counter this type of fraud, all the banks would need to share, in real-time, information about IP addresses, email addresses, telephone numbers, etc. and ideally have this information checked against similar data held in government databases. Multiple participants noted that data sharing in this case was limited by technical barriers (i.e. banks would need to be quickly sharing personal information onwards into a central repository – that did not exist at the start of the scheme) but also a cultural unwillingness to share commercial information about the banks' business.

In response to the feedback on the Bounce Back Loan scheme, BEIS is working with private sector organisations to bring data together from a wide range of sources to both identify fraudulent loans and additionally support recovery activity. One element of this activity has been to co-produce a product between government and the private sector that can help identify and tackle fraud within the scheme. These initiatives, as one participant explained, have moved the Bank from being a consumer of information from other sources and organisations to being a holder and provider of information to other departments within government.

The Bounce Back Loan scheme highlighted the difficulty of quickly establishing new data sharing agreements between government and multiple financial sector organisations. Participants agreed it would be helpful if there was an established framework for sharing individuals' data, which would have made it realistic to build systems quickly for sharing data with analysts, academics and others to use, but this was not possible to establish during the pandemic. A route for consideration mentioned by one participant would be to run pilot projects, or sandboxes, around what data sharing would be legally and publicly permissible, with industry and government collaborating and agreeing what and how data could be made available in a common secure research environment.

Successful counter fraud examples

Cyber-enabled fraud

Digital services and the data they process must be protected from malicious cyber threats. While all services are required to meet certain security standards, the fast-moving context of cyber threat, and a variety of different approaches to securing services has created an uneven landscape where security can be an impediment to effective data sharing. This can be countered via a common, mandated approach to 'secure by design', which will align the various approaches to securing digital services across government and provide a framework within which security becomes less of an impediment to data sharing whilst services are more secure from cyber attack and fraudulent use. An example threat of this type was the Log4shell attack* of the Log4j system in late December 2021.[4] This exposed a potential vulnerability across computer systems worldwide that used the software logging tool. In response, a scanning tool was built to identify a quarter of a million potential targets across the public sector that may have been compromised. Knowing the number of targets gave a real picture of the scale of the risk involved in the cyber attack and helped those who were compromised mitigate their vulnerability as solutions were developed.

Identity fraud

There are a growing number of services supporting digital identification services and protecting against identity fraud. Proper development of these services requires a trust framework.** DCMS and GDS are working together with private organisations to develop

* The Log4shell vulnerability allowed attackers to remotely run malicious code by changing a standard lookup address on the target machine, which could then leak sensitive information from the network or run a ransomware attack.

** A trust framework is a common set of rules agreed by all involved organisations to ensure that they operate consistently. A framework can include standards, guidance, rules and legislation.

a trust framework to underpin the 'OneLogin' system and others for government. The trust framework will need to establish what data is required to be shared between services/organisations that can simultaneously demonstrate and protect identity information, such as personal identity, address and contact information.

Money laundering

To counter money laundering, a joint money laundering intelligence task force was established in 2015 to share information between law enforcement and the financial sector on organised crime. One participant described how the success of the initiative was due to trust and confidence between different sectors and partners. In the beginning there was lots of apprehension from participating organisations due to the nature of the data being shared, and therefore the process started with caution and proof of concept in the early stages. But after five years of operation, 970 operational cases have been completed and over 4,000 bank accounts identified by law enforcement resulting in 250 arrests. This, the participant stated, was the impact possible when there is confidence and infrastructure in place to share operational data.

Universal Credit

Universal Credit has successfully reduced employment income fraud through the use of data sharing of payroll data via HMRC. However, during the pandemic, certain easements were put in place by DWP on the system to enable faster payments, which led to an estimated £3.5bn increase in Universal Credit fraud. DWP is now using data analytics to identify these cases for manual review. One challenge is that universal credit payments are subject to rules on how much capital an individual has. To prevent fraud in this area, a sharing agreement is required which would allow DWP to request the bank account details of individuals if there is suspicion of fraudulent reporting of existing capital. Such an agreement, which would require matching an individual with accounts in different banks, would require new legislation however.

Improvements to data sharing practice for counter fraud

Participants characterised the government's overall pandemic response as mostly a medical emergency with some financial interventions resulting from it. There was agreement at the roundtable that, with hindsight, some institutional naivety was present in decision making to get financial support to struggling businesses in an unprecedented situation, such as allowing businesses to self-certify for the Bounce Back Loan scheme. This was the case for other initiatives, as well as the scheme, and government took on a degree of risk that would likely not have been acceptable in normal times.

Participants agreed that improved data analysis would have helped inform government responses and strategies. This would require better data, easier data sharing, and the right capabilities in place throughout the system to make the most of data analytics to inform policy decisions. To inform such a strategy, participants agreed that government first needed to know what data it has and consider how to make that more accessible across government and third party organisations and academics for broader analysis.

But beyond this, government would need to work with other sectors, such as financial, for counter fraud activities, to identify the barriers that currently limit data sharing and how to overcome these. This may require categorising different data types, separating personal data from commercial data and considering aggregating data to support pattern identification and other bulk analysis techniques.

Recommendations

Participants drew out several key lessons and recommendations for government, based on their experience from a range of counter fraud activity. These included:

- Counter fraud activity will make greater use of data analytics and machine learning will be a key next step for this. Implementing these methods will require new safeguards and governance to show how ethical considerations have been made and provide public confidence that their data is being used appropriately.
- In order to enable future, rapid data sharing, government should agree and adopt a set of data sharing specifications across common data sets.
- Government should consider more public data sharing with banks, telecoms operators, internet service providers and other technology companies in order to prevent fraudulent activity nearer the point of implementation.
- The civil service should continue to build both data and fraud and error expertise across departments so that it can better manage the data it has and have the expert knowledge available in departments to know what is possible to do with the data for counter fraud activities.
- Government should consider what potential legislation is required for full sectoral participation in counter fraud activities.

Paul Shepley is a data scientist at the Institute for Government
Gavin Freeguard is a freelance consultant and associate of the Institute for Government

References

1 Comptroller and Auditor General, *The Bounce Back Loan Scheme: an update*, National Audit Office, December 2021, https://www.nao.org.uk/reports/the-bounce-back-loan-scheme-an-update/

2 Becket A, 'Introduction of bounce back loan scheme', letter to business secretary, Department for Business, Energy and Industrial Strategy, 1 May 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/891469/200501_AO_Direction_letter_on_Bounce_Back_Loans_Scheme.pdf

3 Comptroller and Auditor General, *Investigation into the Bounce Back Loan Scheme*, National Audit Office, 7 October 2020, https://www.nao.org.uk/wp-content/uploads/2020/10/Investigation-into-the-Bounce-Back-Loan-Scheme-Summary.pdf

4 National Cyber Crime Security Cenre, 'Log4j vulnerability - what everyone needs to know', webpage, no date, https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know

INSTITUTE FOR GOVERNMENT

The Institute for Government is the leading think tank working to make government more effective.

We provide rigorous research and analysis, topical commentary and public events to explore the key challenges facing government.

We offer a space for discussion and fresh thinking, to help senior politicians and civil servants think differently and bring about change.

Copies of this IfG Insight are available alongside our other research work at:

instituteforgovernment.org.uk

enquiries@instituteforgovernment.org.uk

+44 (0) 20 7747 0400 **+44 (0) 20 7766 0700**

@instituteforgov

Institute for Government, 2 Carlton Gardens
London SW1Y 5AA, United Kingdom

January 2023