Sharing is caring?

Could data-sharing improve the support provided to customers in vulnerable situations?

EXECUTIVE SUMMARY

April 2018

University of BRISTOL
Personal Finance Research Centre

Why is data-sharing important?

This report asks whether greater sharing of data between financial services firms can improve their ability to identify and support customers in vulnerable situations. It considers how such data-sharing could work in practice, and presents 'building blocks' for the industry to consider if it is to take forward increased data-sharing.

The report is based on new research which comprised of an **evidence review** of academic papers, research reports and policy documents from sectors including financial services, health, utilities, and government services; an **online survey** completed by 244 members of the Money and Mental Health Policy Institute's Research Panel, who all have first-hand experience of mental health problems; and 18 **expert interviews** with representatives from financial services, the energy and water sectors, the advice sector, and data specialists.

Why is this topic important?

Every day, firms in the financial services industry encounter a large number of customers in situations that may make them 'vulnerable'. These individuals, due to their personal characteristics or wider circumstances, can be particularly susceptible to detriment if the organisation fails to take their situation into account.

At present, organisations usually only become aware of such situations if the customer (or a third party acting on their behalf) tells them about it. This means that if a customer doesn't disclose the situation to any, or all, of the organisations they encounter they will not receive support they may be eligible for.

Data-sharing between organisations may offer a way to ensure the customer gets all the support they need, without requiring them to have the same conversation with multiple different organisations.

Disclosing personal information can be draining – whether it's about a health issue, a bereavement or some other difficult situation.

Rather than having multiple, similar conversations with different firms, what if the first firm that an individual speaks to could simply notify all the others?

Is there a need for data-sharing?

When exploring the viability of any intervention, we should first ask ourselves: is there a need for it?

To answer this question for data-sharing, we begin by considering the frequency with which consumers already disclose information about vulnerable situations to financial firms, and the extent to which they are required to disclose to a number of different organisations.

Our research finds that it is not uncommon for consumers to disclose vulnerable situations to financial (and other) organisations:

- 44 per cent of respondents in our survey have told their bank about their mental health condition; 38 per cent have told other lenders; and 63 per cent have told a money or debt adviser.
- Over a quarter of those surveyed had told more than one lender about their mental health problem (26 per cent), or more than one money or debt advice organisation (also 26 per cent).
- Our previous research found that debt collection staff receive a median of 15 disclosures of a serious physical illness from customers or their families each month, 12 disclosures of a mental health problem and nine disclosures from a bereaved customer or third party.

In other words, there may be a large number of consumers who are already disclosing sensitive information about vulnerable situations to financial services firms. These individuals and their families could be affected by any move towards greater data-sharing.

44 per cent of those with mental health problems that we surveyed had told at least one bank about their condition and 38 per cent had told at least one other type of lender.

Over a quarter (26 per cent) of all those surveyed with mental health problems had told more than one lender about their condition.

What are the benefits and risks of data-sharing?

As shown in Table 1 on page 5 there are a range of possible benefits associated with increased data-sharing, but also a number of risks that would need to be mitigated against in the design of any data-sharing scheme.

In terms of benefits to consumers, increased identification of vulnerability by firms could lead to more consumers receiving relevant help and support from organisations, or products more tailored to their needs. Data-sharing may also mean that fewer consumers would have to explain their situation to multiple firms, something that our research shows can be very challenging – as evidenced by the fact that 67 per cent of respondents to our online survey found it 'very' or 'quite difficult' to disclose their mental health problem to their bank, as did 65 per cent of those who disclosed to another creditor.

From our expert interviews, it was clear that financial services firms also recognise the benefits of data-sharing and are interested to explore opportunities and learn from other sectors. At the same time, they are understandably nervous about how sharing such sensitive data would work in practice and acknowledge the risks of such data being mismanaged or misused.

Ultimately, there are trade-offs associated with increased data-sharing. The majority of our survey respondents (84 per cent) said that – providing certain conditions were met – they would be open to firms sharing information with other firms about their mental health condition.

Our survey showed that 67 per cent of consumers with mental health problems find it difficult to disclose their mental health problem to their bank.

"Having to explain to banks/ other people you don't know but you are forced to explain is very stressful and unnerving… I come away feeling guilty and angry with my past… it made me feel suicidal." **(Survey respondent)**

84 per cent of consumers with mental health problems would be open to firms sharing more data with one another – providing certain conditions are met.

What are the benefits and risks of data-sharing?

Table 1 - Potential benefits and risks of data-sharing

	FOR INDIVIDUALS	FOR ORGANISATIONS
POTENTIAL BENEFITS	• Customers receive additional support from firms, more tailored to their needs • Customers spend less time and effort disclosing information about their vulnerable situation • Minimises emotional impact of multiple disclosures	• Greater regulatory compliance • More sustainable arrangements reached with customers • Overall reduction in time-cost of calls for organisations • Improved customer satisfaction
POTENTIAL RISKS	• Poor-quality data is recorded and shared • Error in data use, interpretation, storage that creates detriment • Exclusion from the market or from extra support • Exploitation by unscrupulous firms • Exposure to frauds and scams	• General Data Protection Regulation (GDPR) non-compliance • Data breaches • Misuse of shared data • Costs of new systems and processes

Source: authors' summary of evidence and interviews with stakeholders

Five building blocks for greater data-sharing

The evidence suggests there may be considerable benefits to data-sharing but also highlights risks that need to be managed correctly. Drawing on other sectors' experiences, to examine how such a system might work in practice we considered five building blocks for greater data-sharing:

1. **Data disclosure** – organisations first need to consider ways of encouraging consumers to proactively disclose information about vulnerable situations to them. Crucially this involves creating an environment in which the consumer is comfortable and explaining why this information may be required.
2. **Data capture** – vulnerability is often complex, multi-faceted and episodic, which makes it difficult to neatly categorise in the binary way usually favoured by digital systems. Firms therefore need to consider how to capture data in a standardised way, if data-sharing is to work.
3. **Data hygiene** – data-sharing requires the introduction of systems to ensure that data is error-free and up-to-date, especially where consumers are affected by short-term or episodic vulnerabilities.
4. **Data sharing** – here we present a number of different models of data-sharing and new technology that could enable such a system to work in practice.
5. **Data control** – regardless of the system used to share data, it is of fundamental importance that the consumer retains control over their data and is able to change or delete the information stored about them, as required.

1. Data disclosure

For data-sharing between organisations to be effective, consumers first need to disclose this information to the organisation or at least give their consent for existing data held about them to be disclosed by one organisation to another.

From our consumer survey, disclosure by consumers with mental health problems is not uncommon. Yet significant numbers of people do not disclose information about their mental health; and this may well apply to other vulnerable situations as well, such as substance addictions, gambling problems or domestic abuse. There already exist tools and protocols to help financial services staff deal appropriately with customer disclosure. Some of our industry experts felt that encouraging more customers to disclose information about their vulnerable situation to firms (and ideally to disclose it earlier) would be a useful first step towards greater data-sharing.

What's happening in other sectors? Working with the energy sector, Citizens Advice plans to create a universal and accessible online registration process for the Priority Services Register (PRS) to make it easier for energy customers to apply for non-financial support services.

In the gambling industry, people can ask to be self-excluded from all Licensed Betting Offices that they use or are likely to use, under the Multi-Operator Self-Exclusion Scheme (MOSES) – although the scheme's effectiveness has been questioned.

Five building blocks for greater data-sharing

2. Data capture

Financial services firms have well-established systems and processes for capturing customers' financial transaction data and sharing it e.g. with credit reference agencies. Capturing data about someone's (non-financial) vulnerable situation is a very different prospect and one that provoked a lot of discussion in our expert interviews.

Defining vulnerability from an operational perspective was seen as a vital first step towards greater data-sharing, but one that is challenging not least because of the wide spectrum of different vulnerable situations and the various degrees to which they may affect individuals. Under GDPR, the collection of personal data should also be "limited to what is necessary", rather than "not excessive" (as in the Data Protection Act).

One solution might be a standard classification of vulnerability that provides more information than a simple vulnerable/not vulnerable flag and can help firms decide their own intervention or 'treatment' strategy. Even if a standard classification does not completely negate the need for further contact with a customer, it might assist a more outcomes-focused conversation. It was clear from our research that any new plans for greater data capture and data sharing would have to work within the constraints of organisations' existing information systems.

What's happening in other sectors? The energy sector has worked through similar issues regarding vulnerability definitions and classifications. An industry-led group has, over the last two years or so, worked together to develop a set of standardised vulnerability Needs Codes (the categories that allow customers to register on the Priority Services Register for additional support) that are being rolled out across electricity and gas companies. The Needs Codes cover particular circumstances and conditions (e.g. people who are dependent on medical equipment, or who have poor mobility, communication difficulties or mental health problems), which are perhaps more prescriptive than the wider understanding of vulnerability that exists in financial services.

3. Data hygiene

Data hygiene means making sure that data is relatively error-free. For personal information about vulnerability, our expert interviewees focused in particular on the importance of maintaining accurate and up-to-date data in the interests of customers, and in line with data protection law.

For relatively stable long-term circumstances or situations, this may be fairly straightforward. However, a vulnerable situation might well be episodic or transitory which makes data hygiene more challenging. In these situations, how can organisations maintain accurate data (including removing data if customer consent is withdrawn)? One way is an outbound customer contact programme run by the organisation that holds the data. For individual firms to run their own customer contact programmes could be costly and duplicative, and almost inevitably involves a time lag between the customer disclosing new information and their records being updated. On the other hand, if they

Five building blocks for greater data-sharing

rely on inbound customer communication, firms' may well end up with out-of-date vulnerability data.

What's happening in other sectors? In the energy sector, there are temporary Needs Codes (such as post-hospital recovery) that enable customers to join the Priority Services Register for non-financial support. According to our expert interviews, energy companies are expected to update and clean their register data periodically. For temporary Needs Codes, this might involve contacting the customer to check their situation; expiring the data according to a pre-agreed time period; or leaving the code in place until the customer contacts their supplier in the normal course of business.

4. Data-sharing

Most private and third sector organisations already have a general ability to share information, provided this does not breach data protection or any other law. We looked in detail at three possible models for organisations to share more data about customers in vulnerable situations. Any data-sharing model can only be as good as the information that organisations record, however, and their systems for data collection, use, storage and sharing.

Model 1: Company-to-company sharing. Company A receives information from a customer about their vulnerable situation and shares this with other firms as agreed with the individual and in line with data protection law. An example of this data sharing model is the Priority Services Register that operates in the energy industry.

Model 2: Customer-facing vulnerability register. An individual in a vulnerable situation adds their details to a third-party database (or someone with Power of Attorney does it for them). Companies either search this database or are automatically updated about the customer's situation, in line with data protection law. An example of this data sharing model is the Vulnerability Registration Service.

Model 3: Third-party inter-company database. Company A receives information from a customer about their vulnerable situation and shares this with a third-party database provider, in line with data protection law. Other companies can be notified if one of their customers is added to this database or they can search the database themselves. An example of this data sharing model is a credit reference agency.

Another option might be for individuals to share vulnerability information via the Notice of Correction system operated by credit reference agencies (where individuals can add a note to their credit file if they want to provide an explanation or feel something is misleading). However, in their current form NOCs may not provide an optimal way of recording and sharing vulnerability data for data capture and data hygiene reasons.

A different approach might be to use blockchain technology. Blockchain is an encoded digital ledger that is stored on multiple computers in a network that exists without a centralized authority or server managing it. This new technology could offer another way for individuals and organisations to securely share personal data - and allow individuals

Five building blocks for greater data-sharing

close control over the ways in which their data are shared and used. For example, at any given time an individual may alter the set of permissions for their data and revoke access to previously collected (or shared) data.

5. Data control

The preceding building blocks have mainly considered data control from an organisational perspective. But what about personal control over data-sharing and data use? In a 2011 publication, the World Economic Forum noted the emergence of personal data services which "… *provide the safe means by which an end user can store, manage, share and gain benefit from his or her personal data*."

With a personal data service, an individual's identity is validated and assured, reducing the risk of fraud for the end-user and the organisations that they share data with. It can also simplify data management, for example by doing away with the need for multiple passwords.

An example of a personal data service in the UK is Mydex, a Community Interest Company. Mydex users can choose what data they want to store and potentially share. They can also create their own set of verified proofs about their situation (e.g. their identity) and store a verified copy of the data which they share and manage themselves.

Among our expert interviewees, there was also interest in the opportunities that Open Banking might offer to help people manage their own data – initially financial transaction data, but potentially also vulnerability data. An individual might, for instance, be able to give an aggregator service access to their data, that could then be on-shared with other organisations as determined by the customer, for example via a data dashboard where they could switch access to their data on or off. This, of course, raises a practical question about whether customers in vulnerable situations are always able to exercise 'data control' in their lives, due to their vulnerable situation making it more difficult.

Steps towards greater data-sharing

Steps towards greater data-sharing

While certainly challenging, our expert interviewees did not want to relegate vulnerability data-sharing to the 'too difficult pile'. So what are the next steps towards greater data-sharing among financial services organisations? Our research suggests three possible steps:

- For firms to look at ways to achieve better data-sharing *within* their own organisation or corporate groups – a significant issue, according to our expert interviews.
- To undertake proof of concept work; for example, pilots to share data for one type of vulnerability, such as one or more long-term health conditions or disabilities.
- To explore the feasibility of a shared way of classifying vulnerability.

If individuals or organisations want to take these (or other) steps forward, we believe our research findings offer a useful starting point.

The data-sharing debate is still at an early stage. As GDPR comes into force and technology continues to advance (bringing down the costs of infrastructure changes), we should see more opportunities for data to be used as a force for good, for the benefit of consumers and firms.

This research was carried out by the Personal Finance Research Centre, University of Bristol. The Executive Summary and Research Report are authored by Professor Sharon Collard (Research Director), Jamie Evans (Research Associate) and Chris Fitch (Honorary Research Fellow).

Acknowledgements We thank Barrow Cadbury Trust for grant funding this project; the Money and Mental Health Policy Institute for giving us survey access to their Research Community; the Research Community members who kindly completed the survey; and the industry and consumer experts who gave up their time to be interviewed.

University of BRISTOL
Personal Finance Research Centre

Barrow Cadbury Trust