

Data Sharing Review

Richard Thomas and Dr Mark Walport

Consultation paper on the use and sharing of personal information in the public and private sector

List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to contact@datasharingreview.gsi.gov.uk

Alternatively you can send a hard copy response to:

Data Sharing Review Secretariat
5.26 Steel House
11 Tothill Street
London
SW1H 9LJ

Thank you.

Section 1: Background

Question 1.

Comments: The FSA's primary interest in data sharing/protection is to ensure that the financial services firms we regulate have appropriate systems and controls in place to minimise the risk of personal information being obtained and used by criminals. Indeed, there is a specific rule in the FSA Handbook (SYSC 3.2.6R) which requires firms to have in place adequate systems and controls to prevent financial crime. In addition, we expect FSA-authorized firms to comply with all relevant non-FSA legislation/regulations including the Data Protection Act.

In order to ensure that firms are holding their customers' data securely, we have conducted a significant review of a range of firms' data security controls and are due to publish our findings in Spring 2008. This review is referred to as the "Data Security Review" in the remainder of our response.

A related concern of ours is the way in which non-financial services firms' data security systems and controls are regulated. It appears that the sanctions and powers of the FSA exceed those of non-financial services regulators, including the Information Commissioner's Office. In our view, this may lead to poorer standards of data security in non-financial services firms. This, in turn, could lead to the targeting of the non-financial services firms by criminals seeking to

acquire personal information in order to commit fraud and/or identity theft. .
One likely use of the stolen data will be to commit fraud in the financial sector,
so we are interested in this indirect risk.

Finally, we would like to emphasise that the FSA believes that no changes to the current
regime should be introduced without a full cost benefit analysis, market failure
analysis and public consultation. In addition, the ICO should have regard to
the Government's better regulation principles.

Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2.

Comments: N/A

Question 3.

Comments: As stated above, our main concern is that data sharing - if not well controlled -
could lead to personal information falling into the wrong hands and being used
for criminal purposes such as fraud and identity theft.

Question 4.

Comments: The main risks identified during our Data Security Review in relation to data
transfer are as follows:

- A lack of due diligence by firms of third party service providers to whom data is transferred or with whom data is shared. Inappropriate reliance is placed on assumptions that contractual terms are being met with very few firms appearing to conduct proactive checking of important aspects of data security at third parties such as how staff are vetted; exactly which staff at the third party have access to the data, technological controls (eg encryption) in place to protect data at the third party; and physical security at the third party firm. Some firms which demonstrate good practice in this area conduct regular audits of third party suppliers to ensure that they are holding information securely. A particularly high risk is the lack of security in some firms' data back-up processes. As you know, firms should back up their IT systems on a frequent basis to ensure that data is accessible in the event of an unexpected event such as a fire, flood or IT breakdown. However, we have seen examples of where copies of firms' entire customer databases are stored offsite with third party service providers and there is very little or no understanding of the security arrangements in place around this data.
- Poor standards of data transfer: Most large and medium sized financial services firms now transfer data to and from third parties using secure internet links but there are still occasions where media such as CDs or USB storage devices are used. Our experience is that these media are not always encrypted and, on some occasions, are sometimes sent by unrecorded post. We would expect transferred data to be encrypted to a reasonable standard and for any media sent by post to be recorded/traceable and sent to a relevant named individual. In addition, we have seen instances of surplus data being transferred to third parties where firms consider it inefficient, difficult or time

consuming to restrict a dataset to just the information required for a particular task. This would often expose consumers to increased risk of financial crime in the event of a data compromise.

- In some firms, there is a general lack of awareness that customer data is a valuable commodity for criminals. Training for front-line staff, who often have access to the greatest volumes of customer data is rarely relevant to their day-to-day duties and focuses more on legislation and regulation than the risk of financial crime. As a result, staff are often not aware of why following data security procedures is an important tool for reducing financial crime. In addition, many firms do not test that their staff understand their policies.

Question 5.

Comments: N/A

Question 6.

Comments: N/A

Question 7.

Comments: N/A

Question 8.

Comments: N/A

Section 3: The legal framework

Question 9.

Comments: N/A

Question 10.

Comments: N/A

Question 11.

Comments: N/A

Question 12.

Comments: We believe a significant strengthening of the ICO's powers and resources is essential in ensuring data security, as well as compliance with other aspects of the Data Protection Act, across both the private and public sector. We understand from useful discussions with the ICO that they do not at present have the power to inspect an organisation's systems and controls without the organisation's consent, nor can they fine organisations for serious breaches of the data protection principles. We would strongly support a change in legislation which would give the ICO such powers. This would ensure a level regulatory playing field across the public and private sectors. At present, financial services firms face greater potential regulatory sanction for data security breaches as the FSA can both inspect financial services firms without consent and impose fines where an investigation shows that the FSA's rules or principles have been breached. As an example, the FSA fined the Nationwide Building Society almost £1mn for data security weaknesses in February 2007 but non-financial services firms cannot be fined for similar breaches, despite a number of high profile cases.

Question 13.

Comments: N/A

Question 14.

Comments: N/A

Question 15.

Comments: N/A

Section 4: Consent and transparency

Question 16.

Comments: We have seen examples where customers' consent to data sharing is obtained by default (eg a customer must tick a box if he DOES NOT want his data to be shared with a third party). The ICO might wish to consider, if it is not already, that customers should 'opt in' to any information sharing arrangement. In addition, it might wish to consider whether firms should make clear who data will be shared with. We often see small print which states that information can be shared with 'selected third parties'. This is not particularly transparent for the consumer and could give rise to financial crime risk. For example, if a customer's bank shares information with an unnamed third party and a data loss occurs at that third party, there would be a risk that the customer might think he is not affected.

Question 17.

Comments: N/A

Question 18.

Comments: N/A

Question 19.

Comments: N/A

Section 5: Technology

Question 20.

Comments: Technological advances mean that data can now be transferred faster, more efficiently and in greater volume. While this results in significant efficiency gains for businesses, there is, unfortunately, an increase in the risk of bulk data falling into the wrong hands if it is not properly managed. Firms should have in place appropriate systems and controls to prevent the malicious or accidental compromise of the data they hold. For example, access to bulk information should be restricted to an individual's needs and firms should consider appropriate controls around portable media (eg lockdown or encryption of portable media) and data sharing/transfer.

Question 21.

Comments: In our view it would be difficult for the law to mandate specific technical safeguards for protecting personal information as technology is evolving so quickly. For example, a certain level of encryption might be appropriate now

but not in a year's time. We would therefore recommend that any change to the law should state that there should be 'reasonable' or 'appropriate' technical safeguards in place. The ICO - or other relevant body - could then issue guidance to the industry on its interpretation of what 'reasonable' technical safeguards are and update this guidance as required.

Question 22.

Comments: N/A

Section 6: International comparisons

Question 23.

Comments: N/A

Question 24.

Comments: California's Senate Bill No. 1386 ("SB 1386"), requires any company that stores customer data electronically to notify its California customers of a security breach to the company's computer system if the company knows or reasonably believes that unencrypted information about the customer has been stolen.

We believe that consumers should be notified in the event of a data security breach - unless there is law enforcement or regulatory advice to the contrary - so that they can take measures to protect themselves from fraud, identity theft or other crime. Your data sharing review might wish to consider whether legislation of this type might be appropriate in the UK.

Question 25.

Comments: N/A

Question 26.

Comments: N/A

Section 7: Additional questions

Question 27.

Comments: N/A

Question 28.

Comments: N/A