



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

Date: 14/02/2008

Dear Sirs

CONSULTATION ON THE USE AND SHARING OF PERSONAL INFORMATION IN THE PUBLIC AND PRIVATE SECTORS

1. The FLA (Finance & Leasing Association) welcomes the opportunity to respond to the Data Sharing Review.
2. The FLA is the principal representative of the asset finance, consumer finance and motor finance sectors in the UK. FLA members provided £93 billion of new finance to business and individual consumers in 2006. Over £65 million was provided direct to consumers (including around 30% of all unsecured lending and 50% of all new car registrations), and £27 billion to businesses and public services, representing nearly 30% of all fixed capital investment in the UK (excluding real property).

The FLA and data-sharing

3. The processing of personal information is crucial to the credit industry. Properly organised and controlled data-sharing enables lenders to make responsible lending decisions. It is clearly very important that the personal data involved is properly protected and handled so as to minimise the opportunity for fraud. The credit industry has a well-developed system for doing so, described in the rest of this paper.

Background

4. FLA members collect and store personal information relating to their customers. This is done to the extent necessary to process an application for credit, to provide credit to the customer, and to service the credit agreement during its lifetime.
5. Certain elements of this information are shared between lenders via the credit reference agencies (CRAs). These include name, address, date of birth, and payment profile. Sharing this information enables other lenders to gauge an individual's level of indebtedness and thus take responsible

lending decisions. For this reason, consumer advocacy organisations support the sharing of information for these purposes. The shared information is also important in verifying an individual's identity, managing risk and minimising potential bad debt.

6. FLA members may also share information on an individual with CIFAS (the UK's Fraud Prevention Service) if that individual has undertaken a proven fraud. This is important in enabling other lenders to identify potential fraudulent applications.

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

7. There are many benefits to sharing personal information in the credit industry. These include:
 - The wide availability of credit across all sections of the population.
 - Protection from fraud, money laundering and other criminality.
 - Prevention of overindebtedness.
 - Responsible lending.
 - Speedy responses to credit applications.
 - Minimisation of errors in processing applications.
8. The FLA would therefore strongly oppose any change to legislation which adversely affected the industry's ability to share data for these purposes.
9. The industry fully recognises that data about individuals must be properly protected. In particular, the risks of identity fraud and money laundering must be guarded against. The credit industry bears a high proportion of the costs of identity fraud and is therefore involved in a significant number of initiatives to prevent it. These include the CIFAS Fraud Prevention Liaison Group, the Joint Money Laundering Steering Group, the Association of Chief Police Officers' Economic Crime Portfolio Group, and the Home Office Identity Fraud Steering Group.
10. There is no evidence that this type of fraud occurs because of weaknesses in data protection legislation. Most instances involve unscrupulous behaviour on the part of fraudsters and/or carelessness in the protection of personal data.
11. The credit industry takes great pains to hold data in a safe and secure manner. It holds no more than is necessary to service individuals' accounts. The industry invests considerable time and money in training on and compliance with the Data Protection Act. The industry's commercial success is dependent upon the effective and safe processing of personal information. The industry's procedures are robust and kept under constant review.

12. The industry is concerned, however, about the ease with which individuals can update Directors' details held by Companies House. At present, there is no requirement for such changes to be verified. In consequence, false Directors details are often used to perpetuate fraud. We would urge the review team to consider how far Companies House's current procedures are properly compliant with existing data protection legislation.
13. There are also a number of instances where we believe that sharing of personal information would be beneficial but where it is not currently possible. For example, access to certain public sector information would enable lenders to make a fuller assessment of an individual's level of indebtedness and so improve responsible lending. This information includes:
- student loans data;
 - data allowing verification of an individual's income, possibly from HMRC;
 - information relating to council tax and utilities arrears.
14. Similarly, other public sector information would enable lenders to verify an individual's identity and so help prevent fraud and money laundering. Examples include online verification of driving licences via the DVLA and passports via the Home Office. A good best practice precedent is the recent Disclosure of Death Registration Information scheme. Under this, the Registrars General for England and Wales, Northern Ireland and Scotland can disclose death registration information to assist in the prevention, detection, investigation or prosecution of offences, once an organisation has met their strict access criteria. We believe this approach could be applied more widely.
15. As the review team is aware, the industry is also working with the Department for Business Enterprise and Regulatory Reform (BERR) on access to data relating to credit accounts which came into being before the consent clauses were introduced into credit agreements. Again, access to this data would improve responsible lending decisions by giving a fuller picture of an individual's level of indebtedness.

The legal framework

16. On the whole, the industry is comfortable with the way the Data Protection Act (DPA) works. We believe that the Act is effective in protecting individuals' data. When sensitive information is mishandled, the Act is clearly breached, showing that it is pitched about right.
17. Given the level of resource which FLA members invest in compliance with the Act, any changes would be extremely costly to implement and should therefore be avoided unless there is a clear cost-benefit justification for them, in line with the Government's Better Regulation principles.

18. The credit industry takes very seriously the second principle of the DPA (*Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes*). The industry established the Steering Committee on Reciprocity (SCOR) specifically to develop and oversee guidelines on the use and sharing of credit performance and related data about individuals.
19. SCOR developed the Principles of Reciprocity in consultation with the industry and with regulatory bodies. The Principles contain the rules for the recording, supply and access of credit performance data being shared through the CRAs. The governing principle is that data should only be shared for the prevention of over-commitment, bad debt, fraud and money laundering, and to support debt recovery and debtor tracing, with the aim of promoting responsible lending.

Consent and Transparency

20. FLA members are clear about the requirement to obtain an individual's consent before sharing personal information. The FLA provides its members with a standard Fair Processing Notice (FPN) to obtain individuals' consent for sharing information with the Credit Reference Agencies (CRAs) and CIFAS. CIFAS and Experian also produce standard fair processing notices for companies who share data with them.
21. FLA Members also obtain the consent of individuals before sharing information with third parties to the account.
22. Compliance with the FLA's Lending Code is mandatory for FLA members. Section 1G of the Code provides additional requirements in respect of data protection and confidentiality (for a copy of the Lending Code please see www.lendingcode.org.uk).
23. But there are circumstances where access to information is required for fraud prevention purposes, and where consent should not always be necessary. For example, the DVLA will not at present verify or confirm whether a driving licence is valid without the consent of the licence holder. It is clear that a potential fraudster would not consent and the effectiveness of the system is thereby impaired. In these circumstances, finance companies may request an exemption under Section 29(3) of the Data Protection Act, which overrules the need for consent in cases of suspected criminality or forgery. The FLA urges the Government to devote sufficient resource to the handling of these requests. Speed is of the essence in detecting fraud and other criminality.
24. As indicated above, the customer is clear from the outset what personal information will be shared and with whom. Moreover, the information shared by FLA members with the CRAs is transparent and individuals can obtain copies of their credit files from the CRAs for just £2.

25. It would not be practical or sensible to require an individual lender's proprietary credit scoring model to be made publicly available. Apart from the obvious commercial problems, the extra risk of fraud would be substantial.

Technology

26. Technological advances have played an important role in the fight against ID fraud. Software assists the instant verification of identity and in tracing individuals. Instant access to CRA data also enables credit businesses to operate quickly and provides consumers with the immediate credit decisions necessary to keep the market and economy operating smoothly.
27. The seventh data protection principle (*Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*) deals sensibly with the risks inherent in modern portable IT devices. We do not believe that a change to the law is necessary. Organisations should consider carefully their compliance with the existing principle.

International comparisons

28. Through our contacts with our sister trade bodies in the EU and with our European Federations (Leaseurope and Eurofinas) we are aware that the UK has one of the most robust data protection systems in Europe. We would not want to see any regulatory changes that would undermine this position.
29. It would certainly be worthwhile, nonetheless, if there were a single individual identifier in the UK like the US social security number. This would reduce the amount of personal information that companies need to collect in order to verify identity for money laundering and fraud purposes.

Conclusion

30. The FLA and its members are generally comfortable with the way the DPA operates. We do not see a convincing case for substantial change.

31. But more needs to be done to change public perception of how data is used. If the public were more aware of why organizations hold data, the benefits of doing so and the safeguards which surround it, a more balanced debate would result. We suggest that the review team considers an approach to consumer education on data issues to parallel the efforts currently being made in financial education.

Elizabeth Denyer
Policy Adviser

Elizabeth.Denyer@fla.org.uk

020 7420 9612

For more about the FLA please visit our e-politix micro-site at
<http://www.epolitix.com/forums/FLA>