

14th February 2008

Martyn Taylor
Secretary to the Data Sharing Review
5th Floor
Steel House
11 Tothill Street
London SW1H 9LJ

Dear Mr Taylor

I am replying to your letter of 12 December 2007 to Sir Fred Goodwin, Group Chief Executive of The Royal Bank of Scotland Group ('RBS'), in which you invited comments on the Data Sharing Review by Richard Thomas and Dr Mark Walport.

RBS has contributed to and supports the industry joint response from the British Bankers' Association (BBA) and APACS. Nonetheless, RBS welcomes the opportunity to make its own contribution to this debate through this reply. Set out below are the key elements of our response.

Banker's Duty of Confidentiality

Banks are subject to a legal duty of confidentiality as established in case law and reflected in the Banking Code. Strict interpretation of this requirement can sometimes restrain banks from sharing data in circumstances where this would be generally beneficial – such as fraud prevention, credit assessment and so on. It would in our view be useful to explore ways in which greater clarity can be provided on when data sharing is expressly permitted.

Data sharing with public sector bodies and utilities companies in the interests of responsible lending

The availability of personal data from a wide range of sources, including utilities companies and public sector bodies, would enable us to better understand an individual's overall finances and whether it would be responsible to lend further to that individual. Similarly, more information would help us to assess the ability to repay of an individual with a limited credit history.

Non-consensual credit data sharing

Sharing of positive credit account data is a relatively recent development. RBS currently obtains consent for this activity at the time an individual applies for credit-related services, such as a current account or a loan. However, RBS has several million customers who opened their accounts with the Group before we began to obtain consent for this purpose. Without consent, RBS is unable to share positive credit account data on these customers, which may restrict them from future borrowing from other lenders, despite having a good credit history. Equally, it may enable those with a poorer credit history to borrow beyond their means because we or another lender are not aware of the full state of their financial liabilities.

The Government has recognised that this is an issue and the joint BBA/APACS response includes a reference to the industry's response to the DTI (BERR) Consultation on the Removal of Barriers to the Sharing of Non-Consensual Credit Data.

We would welcome a change to the Data Protection Act that will explicitly remove the requirement for consent for the purposes of sharing personal data in the interests of responsible lending.

Data sharing for fraud prevention purposes

Fraudsters use some of the most sophisticated methods to commit fraudulent activity on banks, either through using technology, or simply through gathering sufficient information over time from a range of sources to be able to convince a bank employee they are a genuine customer.

In order to be able to combat fraud, including money laundering and terrorism financing, it is essential that we have the most reliable and up-to-date information to help us identify a potential fraud before it becomes an actual fraud.

We support the industry response calling for greater sharing of relevant electronic information on fraudsters between the UK Identity and Passport Service, the DVLA and the banks. We also seek greater clarity on s29 of the Data Protection Act to enable us to more easily support law enforcement agencies in a timely manner. A faster response time may help the Police resolve more fraud cases.

Greater clarity and detail in specific technical safeguards

The Data Protection Act 1998 offers us flexibility, but by giving that flexibility it lacks clarity in certain quarters. We would not wish to see the flexibility diluted, but we would welcome greater clarity by way of practical, risk-based guidance from the Information Commissioner. With the pace of technical change, we do not believe that mandating specific technical standards through statute is the correct approach.

Legal entity basis of segregation of data

Complex, diverse businesses such as our Group often have product and service propositions that transcend legal entity structures – and our customers are often customers of several entities in the Group. It would greatly simplify appropriate data sharing (whether to avoid excessive lending or merely offer more joined-up customer service) if we could clarify that companies under common control could share data – subject to appropriate controls – for appropriate purposes as though they were businesses within one legal entity.

We would be happy to discuss further any of these key points if this would assist the Review.

Yours sincerely

Stephen Sanders
Group Head of Regulatory Risk