



APACS

Mercury House, Triton Court
14 Finsbury Square
London
EC2A 1LQ

Telephone 020 7711 6200
Facsimile 020 7256 5527
www.apacs.org.uk

Mr Richard Thomas &
Dr Mark Walport
Data Sharing Review
5.26 Steel House
11 Tothill Street
London
SW1H 9LH

Direct line 020 7711 6348
Direct facsimile 020 7628 0927
Email jacqui.tribe@apacs.org.uk

Our Reference JT/Card Payments

14 February 2008

Dear Mr Thomas and Dr Walport

DATA SHARING REVIEW - CONSULTATION PAPER

APACS, the UK payments association, is the trade association for those institutions delivering payment services to end customers. It provides the forum for the UK's financial institutions to come together on non-competitive issues, to develop banking systems for the future and to provide innovation and developments in payments. It is also the banking industry voice on payments issues such as plastic cards, card fraud, cheques, electronic payments and cash. APACS supplies scheme and project management, business consultancy and secretariat services to the UK payments industry.

It is in specific relation to, and on behalf of, the payment card industry that this submission is made. Other aspects of the retail banking business should be covered off in responses received from other trade associations such as the British Bankers' Association (BBA).

Should you have any questions on the views expressed, my colleagues will be happy to expand on the comments contained within this letter at the meeting on 26 February.

Yours sincerely

Jacqui Tribe
Manager, Legal, Regulatory and Schemes
Cards and Fraud Control Division

General Comments

Within the payments environment, a certain level of data sharing is a prerequisite to facilitate the effective operation of payments in general. This is equally true of the cards environment where for a payment to be successfully processed, details such as the payer's card number may be transmitted both at the time the transaction is taking place (in the case of an authorisation request) and subsequently to enable financial settlement to take place.

Over and above the standard messaging of card details to facilitate the payments process, there are a number of instances where the card industry is either directly (through APACS) or indirectly involved in the sharing of cardholder information. This paper discusses these scenarios, explaining the industry's role in the sharing of data and the reason why we support this level of information sharing.

The card industry is fully supportive of the need for personal information to be shared only in those instances where it can be demonstrated that there is value and/or benefit in doing so. In such cases it is a fundamental requirement that data is shared in a secure manner and that robust processes are in place to ensure that the data is managed in accordance with data protection requirements and that it cannot be compromised.

As an industry, we believe that there are clearly identifiable occasions where the sharing of personal data is in the interests of the public as a whole or necessary to maintain the integrity of the payments industry or to protect innocent and/or vulnerable members of the public. It is in these instances that the industry encourages the review team to recognise the importance of sharing of personal data within the provisions of the Data Protection Act.

Industry Specific Examples of Personal Data Sharing

- ***Fraud Prevention***

The industry is working closely with key stakeholders, such as government departments and law enforcement, in the fight against fraud. In the cards arena it is recognised that fraudulent criminal activity is often perpetrated with the intention of funding other illegal activities. In this area the sharing of fraud data across the industry is acknowledged to be an effective tool in maintaining the integrity of the UK payments industry and is also necessary to understand how the profile of the fraudster changes and therefore what actions the industry needs to take to close down fraud opportunities and where it needs to prioritise activity.

The sharing of data is vital and invaluable in the industry's response to tackling fraud and, in addition to the support it provides in prosecutions and convictions, it provides the banking industry with further behavioural data to make informed decisions when, for example, processing applications and dealing with disputed transactions. This enhanced knowledge assists in the prevention of potential fraud losses and misuse of the payments system.

The recent Government Fraud Review has indicated the importance of effective data sharing across public and private sectors in responding to and tackling financial crime, which it is estimated currently costs the UK economy some £14bn each year.

The DCPCU (Dedicated Cheque and Plastic Crime Unit) is a fully operational police unit that was formed in partnership with the banking industry in 2002 as a direct response to the rapid growth in card crime (1999 – 2001), in part driven by a significant rise in the level of organised criminal activity. Through the establishment of the DCPCU, the industry has been able to work with law enforcement throughout the UK with the shared objective of identifying, arresting and convicting large-scale criminals and closing down organised criminal groups. As an expansion of the DCPCU, APACS and its members are developing data sharing protocols to facilitate more effective collation and dissemination of fraud intelligence information through a newly formed joint police and industry venture, the 'Payments Industry and Police Joint Intelligence Unit'. Established specifically to combat banking-related fraud in the UK, the system will provide the industry with a secure and robust reporting mechanism, supporting the industry's long-term fraud prevention strategy.

For a number of years now, the industry has, through APACS, provided an industry hot card file (IHCF). The IHCF is a fraud prevention tool to prevent fraud losses against banks and retailers alike. It provides a mechanism for the sharing of card numbers that have been reported lost or stolen through APACS approved providers and ensures that participating retailers can be alerted to up-to-date information on 'hot cards' with the ability to validate card transactions prior to completion of the sale and, where appropriate, retain a stolen card. The data that is shared on the IHCF is already 'spent' as it will relate to cards that have been reported lost or stolen and will, as a consequence, have been replaced with a new card carrying either a different card number or issue number.

The sharing of fraud-related data in a controlled manner is a pre-requisite to maintaining the integrity of the UK card payments industry.

In addition to this current activity, APACS, together with its members, is working closely with the City of London Police team to help them develop and implement the data sharing initiatives identified in the Fraud Review including the establishment of the National Fraud Reporting Centre and the National Fraud Intelligence Bureau.

- ***Child Pornography***

More recently, the industry has welcomed the change in legislation, through the Data Protection (Processing of Sensitive Data) Order 2006 that enables card providers to receive police data so that they can withdraw cards from individuals where terms and conditions have been broken. The industry lobbied closely with the Child Exploitation and Online Protection Centre (CEOP) and children's charities and worked in partnership with the Department of Constitutional Affairs to achieve this change in the law.

This is an area where the card industry wanted to act in a morally responsible manner but had found itself constrained by legislation. In future where paedophiles have used credit or debit cards to access illegal images online, card providers can be provided with the information necessary to terminate the account contract and withdraw the card used (in accordance with the underlying terms and conditions).

We are working closely with CEOP on this issue as the industry recognises the sensitivity over handling such information and the need to ensure a secure framework for its onward transmission and subsequent use by card issuers.

- ***Credit Facilities***

In the credit (lending) environment, a well-established data sharing process has been in place since the late 1980s. Such sharing is an essential component of the industry's commitment to responsible lending.

Existing and previous (historic) consumer credit data is an essential source of information on the behaviour and performance of a consumer in managing credit. In assessing new applications for credit and also in managing existing facilities (i.e. credit limit changes), the credit industry uses a combination of data supplied by the consumer, known information (from account history) and CRA (credit reference agency¹) data. Not only does this data help in assessing the customer's application, but it can also be used to enhance the performance of predictive modelling. In turn this enables the lender to make quicker and more effective decisions and identify signs of potential over-indebtedness at an early stage.

This shared credit data has been shown to provide lenders with a highly reliable and effective way of making an informed decision about a consumer's ability and willingness to repay a debt.

¹ E.g. Experian, Equifax and Callcredit

Data quality is essential to the effectiveness of the data sharing process and lenders are committed to sharing accurate data and ensuring that the overall quality of the data available continues to improve. Credit data is managed by the CRAs where stringent checks are in place to identify any anomalies.

The UK industry has developed a strong data sharing governance model over many years, the 'Principles of Reciprocity', which is overseen by a body known as the Steering Committee on Reciprocity (SCOR). This model is subject to ongoing review to ensure it remains robust, and is known to be viewed as an exemplar in a number of other countries where similar processes are being adopted. This is particularly important with developments such as the Consumer Credit Directive (CCD) where the sharing of credit databases on a reciprocal basis is supported and/or encouraged.

Opportunities For Further Data Sharing

We believe that in the areas of both responsible lending and fraud prevention, opportunities for additional data sharing exist and should be further encouraged.

The industry can only access banking-related data either through existing relationships with the customer or CRA held data provided by other financial institutions. However, other financial information exists for some consumers that would assist credit card issuers and other lenders in forming a complete picture of the consumer and their ability to repay.

We would strongly encourage consideration of making public records (in particular student loans and utilities including council tax) relating to credit facilities available and APACS is willing to work with all stakeholders to drive this process.

According to the Student Loan Company overall, outstanding debt on student loans amounts to around £21.1 billion (and growing)², - compared to £54.9 billion (and falling) on credit cards. This makes student loan borrowing an increasingly significant proportion of the overall debt picture.

Not only is it important for lenders to be aware of the existence and level of student loan outstanding when someone applies for a new facility, but also how that credit has been maintained. Information on the level of arrears on student loans is not readily available, however it must be assumed that there will be a proportion of student loans that go into arrears and default in the same way as regular banking and credit facilities.

Lenders cannot be expected to make an accurate assessment of a person's ability to manage a certain level of debt if part of the picture is not available to them.

² As at the end of 2006/2007 financial year

The CAB report that they are seeing an increasing number of cases where individuals are having trouble paying utility bills. Although we do not believe the levels of arrears or outstandings to be anywhere near the potential levels of student loan debt, there is still the ability for the consumer to get into debt with their utility bills. This is particularly true in the case of water bills where the water companies do not have the right to disconnect supply to residential premises (even where the account is in arrears)³. Again, for lenders this information assists in forming a comprehensive picture of the consumer's financial position and ability to manage further credit. Whilst the actual level of arrears may not be particularly high, it is equally important for the lender to take into account payment behaviour.

It is also important for the lender to know whether credit card accounts are being maintained in good order i.e. at least the minimum repayment is made, at the expense of one or more utility bills.

We are also working closely with BERR and other key stakeholders in order to reach a satisfactory conclusion on the outstanding issue of the availability of so-called non-consensual data (i.e. relating to accounts (mostly pre-1999) where consent to share data is missing for historic reasons) for the purposes of credit assessment. As an industry we consider that the more information available, the more informed a decision the lender can make. In the case of non-consensual data, the industry has identified a tranche of credit agreements entered into before today's common fair processing clause was widely adopted.

In the case of fraud prevention, fraudsters are becoming ever more sophisticated and no longer restrict their fraudulent activities to one particular sector or method of working. It is therefore essential that the various bodies (whether within the public or private sector) seek to share information as widely as possible to identify fraudulent activity. By way of example, sharing of data between the UK Identity and Passport Service, DVLA and the payments industry would provide a far more comprehensive picture of, and facilitate the identification of, fraudulent activity where it impacts on more than one stakeholder body. We would therefore encourage broadening the sharing of data in the public interest.

In all cases where data is shared either within the industry or between industry and external bodies, it is done so within a clear and robust framework to ensure its integrity and security and at all times in compliance with the Data Protection Act. It is not in the industry's interests to share information unnecessarily. Therefore, as outlined above, all information is shared in the belief that it will assist in the fight against fraud, inappropriate practices or as part of an overall responsible lending strategy.

-oooOooo-

³ Water Act 1999