

Data Sharing Review

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

Question 1

Please explain what your interest in information sharing is.

The Association of Private Client Investment Managers and Stockbrokers (APCIMS) is the organisation that represents those firms who act for the private investor and who offer them services that range from no advice or execution only trading through to portfolio management for the high net worth individual. Our member firms employ around 22,000 regulated staff, they have £340 billion under management for the private investor and undertook just under 19 million trades on their behalf in 2006.

Whilst many individual shareholders either hold their shares in an individual broker's nominee or in a company's corporate nominee administered by a registrar, it is estimated that there remain over 20 million individual certificated shareholdings. Given also that personal information can be intercepted, there remains the opportunity for individuals to try and fraudulently sell shares which they do not own, either by impersonating the bona fide shareholder or by seeking to change the address of the shareholder, obtain a duplicate certificate and sell the holding in their own name. Whilst some of these attempted frauds are "one-offs", others can be targeted at a number of brokers over a given period.

In March 2006, APCIMS, in consultation with its member firms and following contact with the ICO, introduced a data-sharing facility to enable our members to share data on attempted frauds.

If you have an active involvement in personal information sharing, we would be grateful for the following information:

- **What kinds of personal information do you collect, hold and share?**
- **How do you collect, hold and share such personal information?**
- **For what purposes do you collect, hold and share such personal information?**

The information that is collected and held on a database in a password-protected "Members' Area" of the APCIMS website includes;

- The name and address used by the individual attempting to commit share fraud¹;
- The date of birth of the individual;
- The bank account details used by the individual;

¹ Where these are the names and addresses of the bona fide shareholder, there shall be no implication that they have in any way committed fraud

- Where known, the e-mail address and/or mobile phone number used by the individual;
- The company in whose shares the fraud has been attempted/committed;
- The date of the transaction;
- The amount of money involved;
- Whether the police have been informed and if so who;
- The company registrar; and
- **If known**, whether the entry relates to a “victim of fraud” (the fraudster is using the identity of the bona fide shareholder by effectively changing his or her address and then obtaining a duplicate certificate to sell the shares) or an “attempted fraudulent transaction” (a client using their own name but who it transpires has fraudulently acquired the shares from the bona fide shareholder).

Any further information that is relevant to the particular entry can be included in the “notes” at the bottom of the entry. Not all the above information is mandatory. A “Note for Users” is also available for member firms.

The information is provided by member firms by e-mail but it is not circulated to member firms. Instead, they are notified that new information is available on the database and advised to access the information directly using their individual passwords and usernames. There are currently 198 cases on the APCIMS database.

The APCIMS Fraud Reference Service (FRS) has two main objectives:

- To help member firms and registrars prevent share fraud; and
- To gather statistics on the amount and type of frauds taking place to help assess what more the industry needs to do to help reduce it.

Question 2

What in your view are the key benefits of sharing personal information to a) individuals and b) society? Please provide examples.

The key benefit of sharing personal information is to help identify those that are seeking to commit crime, be it identity theft and share fraud in the case of APCIMS and its member firms or other types of criminal activity.

Question 3

What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.

The key risk of sharing personal data is potentially blacklisting an innocent party or damaging his or her reputation, particularly where their identity has been stolen by a fraudster.

Question 7

Please provide examples of cases where you believe the sharing of personal information between two or more bodies would be beneficial, but where it is not currently taking place.

The sharing of personal information would be useful between different financial institutions, particularly where the same individuals are attempting to defraud different firms or sectors within the same industry, in this case financial services. Links between financial services trade associations are the most obvious way. We understand that this would also be beneficial to those such as the City of London police or Fraud Squad who may be seeking to build up a picture of a fraudster's activities.

Please explain as fully as possible why information is not being shared, detailing what the barriers to the sharing of personal information are – e.g. legal, cultural, financial, institutional – and how these barriers can be overcome.

Data is not being shared for a number of reasons: in some cases information is not being centrally collected by the institutions, information is being collected in different ways, and there remain concerns about what data can be shared and the security surrounding the sharing of that data.

It would be useful if greater clarity could be made available to the financial services industry on what data they can actually share and under what legislation they are protected. A template for how institutions can and should share data both in terms of content and format would also be useful.