

Mr Arun Kendall
Industry Policy
Australian Payments Clearing Association
Level 6, 14 Martin Place
SYDNEY NSW 2000
By email: akendall@apca.com.au

Dear Mr Kendall

Request for comment on '*Aspects of Account Switching*' consultation paper

The Australian Payments Clearing Association (APCA) has requested comments on its industry consultation paper entitled '*Aspects of Account Switching*' ('the consultation paper'). The Office of the Privacy Commissioner ('the Office') welcomes the opportunity to provide comment.

The consultation paper seeks the views of the community on issues relating to the processes involved with re-establishing direct credit and debit arrangements when changing accounts from one financial institution to another. The paper seeks to identify if there is a need for the introduction of measures to facilitate or enhance the ability of customers to change direct debit and credit arrangements when switching accounts. Further, the Office understands from both the consultation paper and our discussions with yourself and Mr Stephen Halliday on Wednesday 17 October 2007, that the model proposed takes the form of a third party central registry.

The advice below is intended as policy advice directed at the intent of the proposal as set out in the consultation paper and the possible impact on the privacy of individuals, and is not legal advice.

About the Office

The Office is an independent statutory body whose purpose it is to promote and protect privacy in Australia. The Office has responsibility for the protection of individuals' personal information that is handled by Australian and ACT government agencies, and personal information held by all large private sector organisations, health service providers and some small businesses. The *Privacy Act 1988* (the Privacy Act) regulates how these agencies and organisations handle personal information.

The Office's jurisdiction over APCA and its membership

The Office understands that APCA members are likely to be covered by the National Privacy Principles prescribed in Schedule 2 of the Privacy Act. However, the Office understands that APCA's turnover is less than \$3 million, and accordingly falls outside

the coverage of the NPPs.¹ The Office discusses below that, if APCA chose to serve as a form of central registry, it could usefully consider ‘opting-in’ to coverage of the NPPs.

Privacy considerations for APCA in relation to account switching

Community attitudes to financial information

Research conducted by the Office into community attitudes to privacy, has consistently found that individuals believe that their personal financial information is especially sensitive.² Accordingly, care should be exercised in how such information is handled, to ensure that such handling aligns with community expectations.

While the Office notes a number of potential compliance issues below, it is suggested that an underlying principle to this proposal should be that individuals retain appropriate control over how their personal financial information is handled. For example, individual should not be surprised that their information has been transferred. This may be best facilitated by ensuring that account switching is subject to the consent of the individual.

Part IIIA of the Privacy Act

As you may be aware, Part IIIA was enacted in 1990 to regulate the practices of credit reporting agencies and credit providers in relation to personal credit information. Part IIIA restricts access to the consumer credit reporting system by providing prescriptive regulation and includes criminal sanctions for non-compliance.

In line with this, the Office notes that the proposed account switching model would involve the transfer of account details, including credit information, between organisations. In this regard, the Office suggests that the following issues may be relevant considerations for APCA:

1. Is the organisation a credit provider as defined under *section 11B – Credit providers?*
2. Would the account information proposed to be transferred be considered to be a credit information file under *section 18E – Permitted contents of credit information file?*
3. If both section 11A and section 18E apply, would the account switching activity fall outside the limitations detailed at *section 18L – Limits on use by credit providers of personal information contained in credit reports etc.?*

The Office suggests that APCA may need to make an assessment of whether Part IIIA will apply to it in terms of the central register and the institutions which will be involved in the account switching. This could form a useful element of a Privacy Impact Assessment (PIA) for this proposal. The potential role of a PIA is discussed later in this advice.

¹ Sections 6C and 6D of the Privacy Act provide that a business with a turnover of \$3 million or less is not an “organisation” for the purpose of the legislation and thus not covered by the National Privacy Principles.

² As reported in various community attitude research projects undertaken by the Office – see, <http://www.privacy.gov.au/publications/#R>.

National Privacy Principles 1 and 5 on notice and openness.

APCA members that are covered by the Privacy Act are required to take reasonable steps when collecting personal information to provide notice to individuals of various matters, including the organisations, or types of organisations, to which the organisation usually discloses information of that kind.³ In regard to the proposal, it seems unclear whether disclosures of this type, from one organisation to another, would be “usual”.

Similarly, NPPs 5.1 and 5.2 oblige organisation to be open with individuals about the handling of their personal information, including by making available a document providing policies on such handling. Compliance with those provision will go some way to ensuring that individuals have an appropriate degree of understanding of how their personal information is to be handled.

National Privacy Principle 2 on disclosure of personal information

In addition, before disclosing account information to another financial institution or to the central registry, the disclosing organisation would need to be satisfied that the disclosure accorded with NPP 2.

NPP 2 requires that organisations may only use or disclosure personal information for the purpose for which it was collected, unless a prescribed exception applies. One exception is where the disclosure is for a purpose related to the primary purpose and within the individual’s reasonable expectations (NPP 2.1(a)). Organisations would need to determine whether both elements of this test are met.

Another exception to NPP 2 permits disclosure where it is with the consent of the individual (NPP 2.1(b)). To be valid, consent must be freely given and fully informed. In many cases, organisations may most confidently meet their NPP 2 obligations by relying on this principle through seeking individuals’ consent to the handling practices.

The Office has produced *Guidelines to the National Privacy Principles*, which may be found at: http://www.privacy.gov.au/publications/nppgl_01.html. These guidelines may assist the APCA in assessing some of the privacy implications of the introduction of an account switching central registry.

Third party central registry model

The Office notes your advice that the proposal may adopt a central registry model. Given that such a registry would likely collect large amounts of personal information, the Office suggests that public trust would be promoted by ensuring that such an entity was covered by the Privacy Act. If APCA, or another body not ordinarily covered by the NPPs, were to fulfil this role, then the Office suggests that consideration be given to that body ‘opting-in’ to be covered by the NPPs. If the role is outsourced, then ‘opting-in’ to coverage could usefully form an element of the contract.

The ‘opt-in’ mechanism is prescribed in section 6EA of the Privacy Act. More information of this provision is available from the Office’s website at <http://www.privacy.gov.au/business/register/index.html>.

If the registry is not covered by the NPPs, either by section 6EA or by normal jurisdiction, the Office suggests that it would be good privacy practice to consider such matters as the period for which the information is retained. In general, privacy is promoted where personal information is only retained for as long as is necessary.

³ See, NPP 1.3 and, for collections from third-parties, 1.5.

Further, limits should be imposed restricting the use or disclosure of this information for other purposes, and robust security measures applied.

Privacy Impact Assessment

The Office encourages organisations that are considering proposals that involve the handling of the personal information of large numbers of individuals to consider conducting a comprehensive PIA at the initial proposal stage.

The *Privacy Impact Assessment Guide* ('PIA Guide') released by the Office in August 2006 is intended to assist Australian and ACT Government agencies in determining the impact new proposals could have on privacy. While our PIA Guide is targeted at government agencies, the core principles can be readily applied to and used by private sector organisations.

It is our view that the APCA could benefit from using our PIA Guide to identify and analyse privacy impacts during the proposal's design phase. The PIA Guide may assist APCA, and other organisations involved, to integrate privacy into the project by working through some practical steps that will:

- identify and define the project scope and aims;
- describe and map the flows of personal information within the project;
- identify and analyse how the project may impact on privacy; and
- consider options to improve privacy outcomes.

In this case, a PIA may also assist the APCA to determine whether legal advice would be necessary regarding the applicability of Part IIIA to the proposal.

Once this analysis is complete, a PIA report can be produced summarising the information and making recommendations about how the privacy impacts and project aims can be successfully managed. A copy of the PIA Guide is attached and is also available at <http://www.privacy.gov.au/publications/PIA06.doc>. There are also a number of organisations that provide specialist advice about privacy and particularly about PIAs. A list of these organisations can be found on our website at <http://www.privacy.gov.au/links/service/index.html>

The Office hopes that the APCA finds these comments useful.

If you have any further enquiries, the contact officer is Linda King, who may be contacted on (02) 9284 9820, or LindaKing@privacy.gov.au.

Yours Sincerely

Andrew Hayne
Acting Director, Policy
Office of the Privacy Commissioner

November 2007