Senator Brett Mason
Chair
Senate Standing Committee on Finance and Public Administration
Department of the Senate
PO Box 6100
Parliament House ACT 2600

28 February 2007

Dear Senator Mason

Thank you for the opportunity for the Australian Smartcard Users Forum (ASUF) to present this submission to the Standing Committee on Finance and Public Administration's Inquiry into the *Human Services (Enhanced Service Delivery) Bill 2007*.

ASUF is an alliance of eight of Australia's leading banks, card scheme operators, card issuers and technology suppliers: ANZ, Commonwealth Bank of Australia, Giesecke & Devrient, Keycorp, MasterCard, National Australia Bank, Visa and Westpac.

As a group, we advocate the benefits of introducing smartcard technology into Australia using common private sector infrastructure. ASUF is therefore broadly supportive of the Australian Government's intention to introduce smartcard technology to the Australian public through the health and social services Access Card.

Since ASUF was formed in mid-2006, the Forum has had very detailed and productive discussions with the Department of Human Service's Office of the Access Card on the introduction of the Access Card.

These discussions have concentrated on the delivery and security of the Access Card information which will be transmitted through existing private infrastructure.

We understand that your Committee will be examining, among other things:

- the Bill's provisions relating to the intended scope and purposes of the card;
- the information to be included in the card register and card's chip and on the card's surface; and
- the range of offences aimed at prohibiting persons requiring an access card for identification purposes and prohibiting other improper uses of the card.

In relation to the intended scope and purposes of the card, ASUF would like further clarification as to whether the legislation may inadvertently constrain the consumer's use of the chip on the card for private purposes.

ASUF believes that the card can and should be widely able to be used for private purposes.

Off-the-shelf applications exist today to store any variety of data on a smartcard securely and to provide hierarchical levels of access to that data. Via the segregation of applications (fire-walling), technology can prevent the access of one application's data space by another application.

This view is supported by a range of research which shows that Australians look forward to greater access to smartcard technology.

Visa research[1] shows that:

- 70 per cent of Australians surveyed believe that smartcards will become an important part of everyday life, and will revolutionise the way we pay for things;
- 64 per cent look forward to having to carry only one payment card in the future and;
- 85 per cent ranked the ability to make safe secured payments, even on the internet, as their primary motivating factor for smartcard use.

MasterCard research[2] shows that most Australians believe that a smart chip on a card improves the security of using that card, and the addition of a Personal Identification Number (PIN) even more so. Nearly 80 per cent of respondents would apply for a smartcard, if able to do so, and 20 per cent would swap service provider should another provider make a smartcard available to them.

This perception is supported by fact: prior to introducing a stringent smartcard program in 2004, Malaysia had one of the highest levels of payment fraud in the world. Fraud committed on Visa cards decreased from 0.74 percent of merchant sales in Q1 2000 to 0.12 percent in Q1 2005. Counterfeit fraud decreased from 0.60 per cent to 0.08 percent of merchant sales over the same period, and in dollar value from $US 400,000 in the year to November 2004, to almost zero by September 2005.

ASUF research[3] shows that more than half of Australians are aware of the Australian Government's proposed Access Card and more than half would

[1] Source Visa research
[2] Source MasterCard research
[3] Source ASUF research

accept its use to be extended to the purchase of public transport tickets and for the payment of calls on public telephone lines.

In reporting on the *Human Services (Enhanced Service Delivery) Bill 2007, the Senate should consider:*

International experience demonstrates that smartcard projects delivered via common private infrastructure can be implemented on time and on budget. A recent national project in Hong Kong of great complexity was delivered on time and under budget. Similar large scale national projects in Turkey, Taiwan and Norway have also been delivered cost effectively and on time.

With regard to protection of the information on the Access Card we can avow that:

- Smartcards provide more security than current systems, as they require significant cost, equipment and effort to break into – more than most are prepared to expend.

  Highly evolved but still low-cost systems for smartcard deployments exist now, to ensure that the cost and difficulty of replicating, counterfeiting or creating fraudulent cards is so high that it becomes pointless to do so. These systems can also ensure that each individual card is so unique that even in the extremely unlikely event that card security keys were compromised, only a single card – and not the entire card base – is at risk. The same theory is equally applicable not just to each card, but to each transaction instigated by each card, ensuring that not only can a transaction not be replayed for fraudulent misadventure, but that each transaction is authenticated, auditable and non-repudiable by the card holder.

- Smartcards lock individual pieces of information separately – only the card holder can allow any information to be shared. There is currently misinformation in the marketplace that privacy of personal information may be at risk with a smartcard. Privacy of personal information is enshrined in legislation in this country, and the smartcard does not change that.

  Smartcards are used extensively around the world to enhance data privacy by providing either (or a combination of):

  - Storage of data in a decentralised manner and held by the people responsible for that information instead of storage in a central database, so that the data on the card can be stored with various access rights and layers of security to reach that information,
    and,

- Unique cryptographic keys, tokens and certificates on each card that only allow access to information stored elsewhere with the permission of the specific card holder.

ASUF would welcome an opportunity to appear before the Committee, as part of its schedule of public hearings in early March.

As Executive Officer of ASUF, I am available to attend a hearing in either Sydney, Melbourne or Canberra.

Please feel free to contact me on 0404 852 813 for any further information relating to ASUF's submission.

Yours sincerely

Jane Mussared
Executive Officer