Supplementary Submission to the Senate Inquiry into the Human Services (Enhanced Service Delivery) Bill 2007 from the Department of Human Services

THE NEED FOR A PHOTO ON THE SURFACE OF CARD

The Prime Minister on 26 April 2006 announced that *"the card will have enhanced security features. It will contain a biometric photograph on the front… in the overwhelming majority of cases it is more than prima facie evidence that the person who holds the card is, in fact, the person referred to on the card."*

In summary, the mandatory photograph on the card is essential to:

- reduce fraud;
- reduce complexity;
- increase customer convenience;
- provide a user friendly and reliable method of accessing Commonwealth benefits;
- improve access to Australian Government relief in emergency situations; and
- permit access card owners to use their access cards for such other lawful purposes as they choose.

This is the object of the Bill.

KPMG has said that it will not stand by the $3b fraud and concessional leakage savings figure if the photo is not on the surface of the card.

The present business case is not based on photographic card readers in doctors, pharmacists and allied health professionals. Our analysis and consultations conclude that this is impractical. Virtually no existing readers in Australia have the capacity to view photographs. While the Human Services' agencies will have this capability, doctors, pharmacists, allied health professionals, specialists, hospitals and third party concession providers will not. To introduce another card reader into a doctor's surgery or a pharmacy will impose an unacceptable burden on their business. (See views of doctors on page 10)

The option of rolling out a huge infrastructure of photo readers is questionable when there is a simpler, cheaper and more secure alternative available, i.e. the photo on the card.

The implementation strategy for the access card leverages existing point of sale infrastructure already available and widely used by most doctors and pharmacists. This technology does not provide photographic images on the terminal. In the absence of an ability to view photographs on the chip in the wider community, the fraud savings from the project are severely reduced.

In the delivery of certain Australian Government benefits and services, such as those delivered by allied health professionals, the card is not expected to be docked. For example, a physiotherapist providing visiting services to a veteran in their home, is not expected to have a reader.

There are situations where even if the technology existed and was fully funded and acceptable to pharmacists and doctors it would not have universal application. For example:

- when there are electricity blackouts and when systems are down
- natural disasters
- home-visiting doctors, including those who routinely attend nursing homes.

Part A – Reducing Fraud

The Australian Federal Police have provided the following material:

> The AFP considers it a necessary security measure for the proposed Access Card to contain a photograph and digital signature on its surface. The inclusion of a photograph on the surface of the card would significantly reduce the opportunity for fraud and identity crime. This is especially the case where a person is required to show up in person to attend a 'participating agency' or where a cardholder presents the card as verification of his or her entitlement to a benefit or service. The provision of a photograph improves the integrity of the verification process. It would enable a person to establish their entitlement quickly and with relative ease. This not only assists the individual but also the agency or person to whom the card is presented.
>
> The AFP-hosted Identity Crime Task Force (ICTF) consists of five law enforcement agencies and has operated for the past three years. Operational experience of the ICTF has shown that documents without photographs or other biometric features are easily counterfeited and reproduced. For instance, the current Medicare card which contains only a name as an identifying feature of the cardholder, is used as a breeder tool to establish an identity and as a means of obtaining more substantial documents to support an identity and commit offences. This is due to its lack of security features. Operational experience has shown that in cases of systematic and organised identity fraud, the one single feature that remains constant in offenders is their facial features. This highlights the necessity and importance of having a facial photograph.
>
> ICTF operational experience has shown that Medicare cards have featured in approximately 35% of their investigations. Fraudulent Medicare cards feature prominently in 70% of the more serious and organised identity crime investigations.
>
> The AFP's Operation Hickey in 2006 resulted in 20 persons being charged in relation to a proven $2.2m fraud on financial institutions in four Australian states. Evidence showed that fraudulent Medicare cards were involved in 90% of the actual frauds committed on the banks.
>
> The Australian Customs Service has reported detection of false identity kits at mail centres. These kits usually originate in South Eastern Asian countries and

are of reasonably high quality. The kits normally consist of a fraudulent drivers' licence, credit cards and Medicare cards.

Of the five most recent investigations by the ICTF involving the seizure of false identity manufacturing equipment, all have included templates for manufacturing Medicare cards on computer equipment along with thousands of blank plastic cards capable of being converted into Medicare or credit cards.

Intelligence gathered over the last three years by the ICTF shows that Medicare cards are an attractive instrument for use by identity crime syndicates because they contain very few security features, and predominantly because of the lack of a photograph or other biometric features. Fraudulent Medicare cards are very cheap to produce because of the absence of a photograph and operational experience has shown that they are also relatively cheap to obtain. The fraudulent document can be reused by various offenders, especially where it is difficult to determine whether the name on the card is female or male, and because of the absence of any information about the age of the person.

The proposed Access Card regime provides greater surety of the link between an individual and relevant entitlements through the enhanced security features, and also protects the individual. The presence of a photograph on the surface of a card provides a basic verifiable link to the person claiming the entitlement, benefit or service.

For the proposed purposes of the Access Card, i.e. the provision of Commonwealth health, welfare, and veterans' entitlements and benefits, it is proposed that card readers or docking stations are used by 'participating agencies' to read the information on the card. While the chip of the card may contain a photograph, which may or may not be able to be read through the card reader, the AFP view is that the surface of the card itself must contain a photograph to enhance its security and reduce the opportunity of fraud and misuse.

The perspective of the Office of Access Card

One of the key reasons for introducing the access card is to reduce fraud and leakage. Fraud savings through the introduction of the access card has been estimated by KPMG conservatively to be $3 billion over the next ten years (see Senate Inquiry evidence). Overcoming this fraud requires the card to have strengthened proof of identity and a photo on the card. The access card incorporates 17 cards and vouchers many of these are concession cards for Australian Government benefits. The access card will also be used to obtain state government and third party concessions. This means that it needs to be robust. Without a photo on the surface of the card it will always be the case that people will be able to get someone else's entitlements as photographic readers will not be available everywhere, every time.

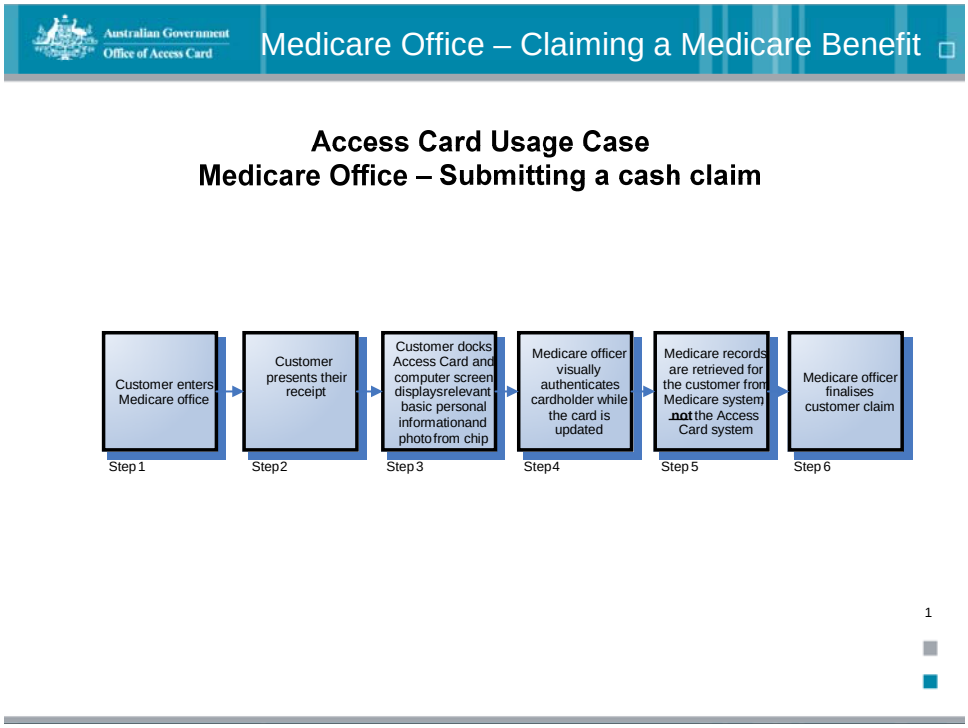
While there will be photographic readers in Medicare Australia, Centrelink and Department of Veterans' Affairs (DVA) offices, readers to be provided by the Government to doctors, pharmacists, hospitals and specialists will not have the capacity to read the photograph in the chip. While it is technically possible to provide such readers, our discussions with pharmacists and doctors indicate that they want readers that they want readers that will fit in with their current business arrangements. They do not see a need for a proliferation of readers and complex interfaces.

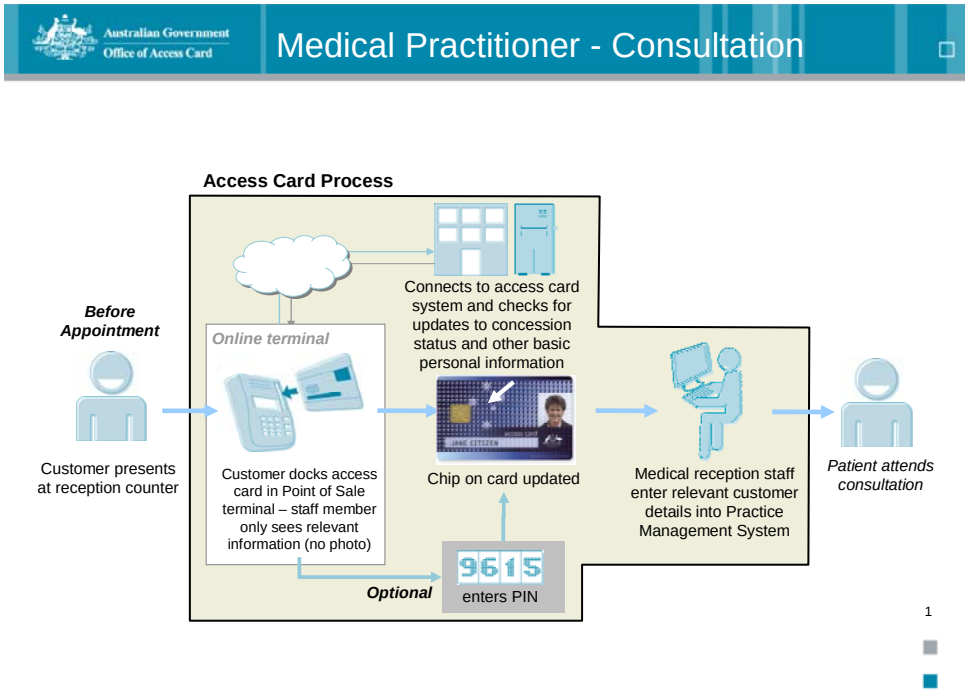
Photographic readers will add to the cost and complexity for customers and business, and remove a major deterrent to fraud. KPMG has noted that it takes considerable bravado to walk into a doctor's surgery and present a card with someone else's photo on it.

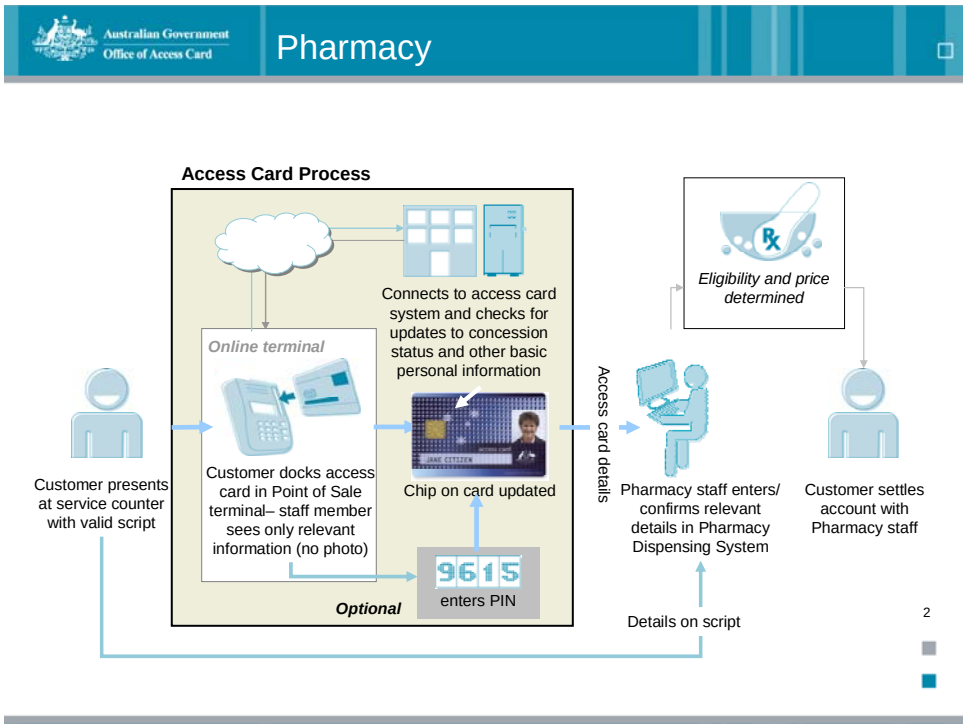
The inclusion of a mandatory photograph on the surface of the card is a key feature of all robust proof of identity documents. In this case, for accessing health benefits, veterans' and social services.

International experience (for example in France and Germany – see summary of relevant international experience at Attachment 1) has shown that where health smartcards have been issued without a photograph on the surface of the card, they have been found insufficient in combating fraud. France and Germany have now moved to issue cards with mandatory photographs. International experience confirms that a mandatory photo on the card is key to having a robust system.

Diagrams 1 to 3 below illustrate how the access card will be used in Medicare (a participating agency), a doctor's surgery and in a pharmacy.







Without a photo on the card, the access card system will be open to fraud. This results in a cost to taxpayers and can lead to a person's identity being stolen and fraudulently used.

Giving customers the choice of having their photograph on the card means that a section of the population who want to exploit the weaknesses currently inherent in the system can continue to do so. Essentially, it will introduce a net with huge holes in it.

Protecting your identity

Contrary to the view that the photograph on the card undermines privacy, having the photograph on the card is a privacy and security enhancing feature. A visible photograph provides a link between a person's name and their identity, thereby reducing opportunities for fraud.

One high profile identity fraud case is that of Jodie Harris, the 'Catch me if you can' thief. Jodie Harris pleaded guilty to about 40 charges relating to identity fraud and theft. She used up to 25 aliases and stole tens of thousands of dollars from scores of victims. The fraud charges she faces relate to Medicare Cards, drivers' licences, passports and credit cards. In at least one case, Harris was accused of obtaining an Australian passport in the name of a victim after stealing that woman's Medicare Card, Qld birth certificate and proof of age card.

Only this week it was reported that a man was charged for possessing a computer that allegedly contained templates for Medicare cards, drivers' licenses and passports.

Without the photograph on the card, a person seeking to establish the cardholder's identity would be forced to either access the person's photograph on the card chip or on the Register or seek other forms of photographic identification. Extending access to the Register is clearly unacceptable on privacy and security grounds. Providing alternative photographic identification is not ideal for reasons relating to security, privacy and customer convenience.

Fraud against the taxpayer

At present concession cardholders (such as those on unemployment benefits) are required under law to present their Centrelink concessions at pharmacies to obtain PBS at a concession rate. In future the access card will replace these cards. PBS concession are already subsidised by the taxpayers but this is an additional concession. The difference in cost for the customer is $25.60 for each and every prescription. PBS concessions account for around $3.3 billion of the $6 billion currently paid through the PBS system.

For fraud to be prevented it is essential for the photo to be on the surface of the card.

Card swapping can and does occur and there is no effective remedy without a photograph. Sometimes, by good chance, Medicare detects a case. For example in 2003, a person was identified in WA using another person's Medicare card to fraudulently obtain narcotics prescriptions in GP consultations. Arrested in June 2003 and charged with 80 counts of fraud, the person received a 12 months jail sentence.

At present legislation requires a pharmacist to request a Medicare number for all PBS subscriptions. Most pharmacists meet this obligation by asking the customer to present their card unless they already know them and have their Medicare number.

If the photo was not included on the surface of the card, and noting that there will not be comprehensive coverage of readers capable of accessing photos, the system would

not achieve the fraud benefits anticipated and the business case for the card would be compromised.

Reduction of Australian Government concession leakage and fraud is premised on the concession or benefit going to the right person and that the benefit is not transferable. Not having the photo on the card basically turns it back into a Medicare Card with a chip. People committing fraud will be able to exploit weaknesses in the system. Of the $100 billion in services and benefits delivered, $20 billion relates to the Medical Benefits and Pharmaceutical Benefits Schemes. It is very difficult to detect cases of fraud in these instances but fraud does occur. For example, recently a person was charged after allegedly using another person's Medicare card to obtain medical services for a relative. The person provided the card to the relative who accessed $10,000 worth of medical care at a Sydney hospital.

The use of Medicare cards to obtain these benefits has been exploited in the past and the incentives for such exploitation have increased considerably with the introduction of the government's new Medicare safety net arrangements. There is an opportunity for people to manipulate and game the system by lending their Medicare card to others in order to reach the safety net sooner, or once they have reached the safety net, to lend their cards to other people who are then able to receive substantial concessions where their entitlements don't exist.

If the coloured access cards that are offered for stable concession groups, such as aged pensioners, eligible self-funded retirees and veterans, do not display a photo they will be an attractive target for people committing fraud, providing almost endless opportunities for significant concession abuse.

KPMG state that a photo is essential for the access card system and that fraud savings could range from at least $1.6 billion to $3 billion dollars over 10 years. The KPMG evidence to the Committee last Friday emphasised that this $3 billion estimate is a conservative one, representing only 0.3% of the one trillion dollars participating agencies will outlay over the period (assuming current funding levels).

Special needs of DVA customers

Most of DVA's business is between the client and medical and allied health service providers. A photo on the surface of the card provides certainty to these service providers about who they are dealing with.

Veterans and war widows have very frequent personal face-to-face contact with a wide range of over 50,000 contracted providers of health and community services. While these are government benefits they are delivered by third parties. There was no expectation that they would require readers with photo capability. The business case was based on them simply having to show their card or have low cost no photographic readers. A large number of these occur in the home or community setting. A photo on the card is added assurance for both the provider and the veteran that the right services are being provided to the right individual (e.g. medication administration).

It goes without saying that there are major mutual benefits to all clients who are frail, confused or have dementia.

Loss of identity security

Identity crime is one of the fastest growing crimes in Australia. Fraudulent Medicare cards are used to establish fake identities. The current absence of photographic identification in the system and the inability to easily and reliably authenticate the identity and concessional status of a person who presents the card provides endless opportunities for accessing services and benefits for which they are not entitled with little or no chance of detection.

The inclusion of a photograph on the card will protect the card owner's identity and significantly enhance the identity security elements of the card.

At present, if you lose your Medicare card, it is very easy for someone to take that and use it to claim benefits in your name. They can even use it as proof of identity to establish such things as bank accounts in order to perpetrate identity theft. The Medicare Card is what the AFP call a 'breeder document' since it can be used to produce higher forms of identity documentation.

The Australian Federal Police Commissioner, Mick Keelty, reported in his 24 October 2006 speech to the AFR Counter Terrorism Summit that:

> "Identity crime has been estimated to cost Australia anywhere between $1 billion and $4 billion annually. Worldwide the cost has been put as high as $2 trillion."

In their testimony to the Senate Inquiry, the Australian Federal Police reported that they anticipated that the access card would result in a reduction in the use of existing welfare cards in the facilitation of crime:

> "For example, the current Medicare card is easy to counterfeit and reproduce owing to the absence of rudimentary security features such as a photograph and signature, and the lack of other technological protections to ensure the integrity of the card's information and security."

While the access card system will employ a range of technological protections, the photograph and the signature are considered *rudimentary* security features by Australia's premier agency for the investigation of identity theft, the Australian Federal Police.

Having the photo on the card offers a strong deterrent to people using your card to claim benefits in your name such as at a doctors surgery in the form of a bulk bill service.

KPMG also considered that a photograph on the card will strengthen customer confidence in the access card system.

Part B – Facilitating access to services

The photo on the card is central to flexible service delivery

Within Human Services agencies a wide range of service delivery models exist. For example, Centrelink services may be delivered from large metropolitan Customer Service Centres or via individual Centrelink agents working and living in remote Indigenous communities. Medicare benefits may be delivered via large metropolitan health clinics or community controlled health services in remote indigenous areas.

Private providers deliver services on behalf of the Australian Government in a wider range of situations, for example, pharmacists and medical practitioners delivering the PBS and Medicare services, as well as allied health professionals delivering services on behalf of DVA.

Any comprehensive identity verification system needs to support the requirements of the various models and the diverse needs of the customer.

The KPMG business case was predicated on a comprehensive system requiring a photograph: on the surface of the card; in the chip; and on the register (for all but with some exemptions).

As outlined earlier, extending access to the Register is clearly unacceptable on privacy and security grounds. Providing alternative photographic identification is not ideal for reasons relating to security, privacy and customer convenience.

Not all participating offices will have reliable access to technology

Having a photograph on the surface of the card will support safe, reliable and efficient customer authentication where technology is not available or is not reliable, including:

- Natural disasters
- Medicare benefits delivered by home-visiting doctors, including those who routinely attend nursing home facilities
- For the 3.5 million allied health services provided to veterans on behalf of the Department of Veterans' Affairs, at a cost of just less than $200 million
- Medicare benefits delivered in rural and remote areas where there is no internet or telecommunications reception, or where connectivity is so slow that reading a card is an impractical interruption to the normal work flow patterns in the business
- Centrelink new claims facilitated by Centrelink agents in remote indigenous communities
- Business system 'down-time' that occurs from time to time in any business situation (including in metropolitan areas) – our computers have to be serviced at some time, but claims don't stop.

Not all terminals will be capable of displaying a digital photo

As has been outlined earlier, if the photo is not on the face of the card, the photo must be read from the chip to confirm the user of the card is in fact who they say they are.

The chip based electronic image can be readily achieved in the majority of Centrelink customer Service Centres, Medicare Offices, and Department of Veterans' Affairs offices.

Without a photo on the face of the card to authenticate the user, a number of unacceptable risks are introduced into the access card system. These include fraud, lack of appropriate terminal infrastructure, increased costs for government and business, and schedule delays (given lead times to upgrade the terminal infrastructure) and negative impacts on transaction times and service quality. The process of transactions in doctors surgeries and pharmacies will be made more complex if photographic readers are introduced. It adds an unnecessary layer of red tape and will require pharmacists to have three systems rather than the two they currently have. Rather then a simple solution of a photograph on the surface of the card and a point of sales system they will have to grapple with three systems increasing their costs.

The Australian General Practice Network (AGPN) has advised that removal of the photograph from the surface of the card would be logistically difficult for general practitioners. This is particularly the case if communications lines were down. It would not be practical for surgeries to have two terminals and it was generally an unattractive idea. AGPN has made the point that how the card works in general practice should be cutting red tape not adding to it. It should enhance the interface between Government for the general practice and the patient.

There will be lower capacity terminal infrastructure at doctors' surgeries and pharmacies

The implementation strategy for the access card system does **not** incorporate the installation of terminals capable of reading and displaying a photo in doctors' surgeries and pharmacies.

Instead, plans for the access card program in doctors' surgeries and pharmacies are to leverage the installed infrastructure base of bank, acquirer and merchant owned Point of Sale (POS) terminals.

The overwhelming majority of these terminals incorporate a text only LCD (black and white) display. These terminals are not capable of displaying a photograph. Some terminals have a LCD display capable of displaying limited monochrome images (160x80 pixels). These displays would also not be capable of displaying a photograph.

Several manufacturers do offer POS terminals capable of displaying a photograph. Examples include the Hypercom Optimum L4100 terminal (see the discussion of reader types at Attachment 2), Verifone MX870 and the Ingenico

I6700. These are high end POS terminals and have been used by some US retailers to display advertising or coupons. Generally, the terminal faces the consumer and can not be easily seen by the healthcare provider or retail clerk.

The cost of these terminals averages about $2,000. Installation is estimated to add an extra 25% to the cost of the terminal.

The Lead Adviser on the access card project, Booz Allen Hamilton, advises that there are few, if any, terminals deployed in Australia with the capability of displaying a photograph.

Cost of upgrading terminal infrastructure

With very few photo display terminals in place, the only option would be for the Australian Government to invest in replacing the existing terminals with new terminals.

The estimated cost of upgrading (including installation) of terminals to agencies, doctors, pharmacies and third party providers is in excess of $700 million and is unlikely to be technically viable or logistically feasible. This is an additional cost to the program.

It is questionable as to why taxpayers should outlay $700 million for this purpose when photos already appear on many cards now, for example, all driver's licences have photos.

The total value of concessions from non-Commonwealth providers is about $4 billion annually and without a photo displayed on the card there is no easy mechanism for mitigating fraud and concession leakage in this sector.

Access to state and territory and third party concessions

Customers value these concessions highly.

The Australian Government through Centrelink and the DVA issue concession entitlement cards to a range of customers. There are around 2.5 million concession cardholders (including 1.9 million Age Pensioners, 0.3 million eligible self funded retirees and 0.3 million Veterans) who will be eligible for coloured access cards. These people are the major users of an estimated $4 billion worth of state/territory and third party concessions provided each year.

A key benefit of the photo on the face of the card to third party providers is the ability to ensure that the person presenting the card is the card owner. Removing the photo from the face of the card will limit the validation options available to these providers to either the chip or online. Accessing the photo via the chip will require a more sophisticated reader than would be needed to just confirm concession entitlement.

In the absence of a photo on the surface of the card, customers may be required to provide other evidence of identity. Providers choosing to confirm online will not have access to the photo stored on the register.

Negative impacts on service delivery at doctors and pharmacies

The Point of Sale (POS) terminals capable of displaying a photograph (described above) would need to be custom designed for use in the access card context. At present, the display screen is pointing to the customer not to the service provider and it is the service provider who needs to see the photo.

In this scenario the service providers would end up having multiple terminals for different purposes – a point of sale terminal for payment transactions, and an access card terminal provided by the government for reading the photo and their own operating systems. This would eliminate one of the benefits of the proposed access card solution of consolidating terminals at the point of the transaction for many doctors and pharmacies (some service provider locations, particularly pharmacies, would under this model require new terminals, given their pharmacy layout). This would also conflict with the streamlined Medicare claiming process that is about to be deployed as described later in this document. We would expect a strong negative reaction from the medical and pharmacy sector because of the proliferation of readers, the reduced space for business and the cost and complexity of systems.

Transaction Times

Use of a digital image stored in the chip rather than a photo printed on the card will increase transaction time. Reading the digital photo from the chip may take from three to ten seconds plus the time to enter the optional PIN. While this does not seem like a great deal of time, in busy service provider locations such delays can add to congestion and wait times. Pharmacists have advised that transaction speed is an important issue especially at lunch time when many customers queue for prescriptions.

Not all providers will elect to use new technology

Even if the Australian Government was to roll out photo capable readers to all pharmacists and general practitioners (at considerable cost and delay to the project), there is still no reasonable way of ensuring that these are actually used by the providers.

This has been demonstrated by recent experiences with trying to encourage health professionals to upgrade information technology systems.

Having the photograph on the surface of the card provides a reliable and quick way to do transactions. If a provider does not elect to use a card reader, they would need to ring up Medicare to confirm a person's entitlement. Having a photograph on the card allows the provider to confirm both that the person is who they say they are and that they are entitled to a health benefit.

In the absence of a photograph as a safeguard, the Australian Government would again remain exposed on a key area of concessions leakage. Any 'holes in the net' present substantial risks to the identified fraud savings because they provide a target for people looking to commit fraud.

Costs to current initiatives

The broad parameters of the access card system have been taken into account by a range of other Australian Government initiatives. Radical changes to the access card business model will have flow on effects and cost impacts to current reforms.

Electronic Medicare Claiming

For example, if alternative card reading devices are supplied to medical practitioners and pharmacists, they are unlikely to be compatible with devices being rolled out by financial institutions for the Electronic Medicare claiming initiative.

This would result in doctors having two card reader devices in operation simultaneously. Doctors will likely see this as introducing inefficiencies into the administration of their practices.

Missed opportunities

If the photo is not to be included on the surface of the card, all of the costs associated with the registration will remain, but the opportunity to offer better protection of identities and the chance to generate substantial savings from fraud prevention and detection and misuse of taxpayer money will have been missed.

As Chris Jordan AO, Chair of KPMG, has outlined to the Senate Committee Inquiry, it is not a question of if but *when* the Medicare card is replaced by a smartcard. Not to have a photograph on the card in the words of KPMG would be a sub optimal outcome and would dramatically undermine key elements of this business case.

The available research suggests:

- Australians are becoming increasingly concerned about identity theft.
- There is also widespread support in the community for activity to reduce fraud of taxpayer money.
- Australians are increasingly likely to hold some form of photographic identification as a matter of course.

The implementation of the access card represents a once-in-a-generation opportunity to implement new infrastructure to meet the current and future needs of the Australian community.

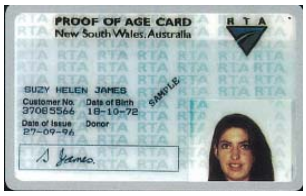
Less convenience for consumers

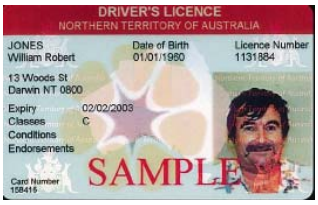
A photo on the surface of the card will allow easy confirmation of card ownership when accessing Commonwealth benefits at frontline service delivery points including doctors, pharmacists, hospitals, specialists and ancillary health care providers by comparing the photo with the person presenting for service.

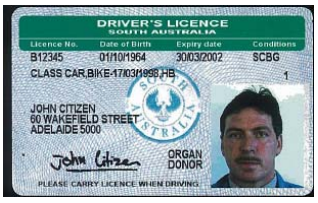
Community acceptance of photo identification

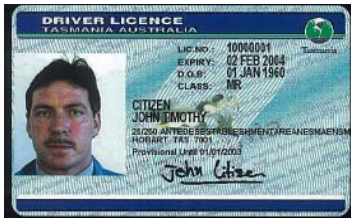
Our market research suggests around 90 per cent of adults have a card displaying a photograph. Photo ID is also common place in many work places, clubs and associations. KPMG has made the point that 'it is not evident why the inclusion of a photo on the face of the (access) card would present additional privacy concerns given the already extensive use of photos in passports, drivers licences and other settings, compared with the enormous benefits that can be gained in terms of service entitlements and anti-fraud benefits.'

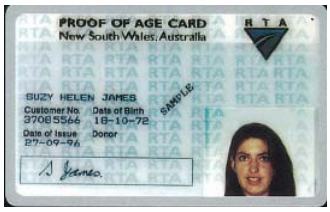
Australian Driver Licence and Proof of Age Cards

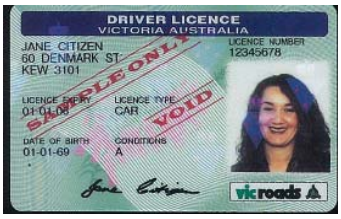












KPMG's view is that a photograph on the surface on the access card will be a major deterrent for fraud.

What the market research says

Qualitative research on the access card has found that most participants wanted the access card to show their name and their photograph.

The research found that the second most commonly identified key benefit of the card (nominated by 80% of people who were aware of the card) was the option to use it to prove identity – especially for people without drivers' licences and passports. The critical issue here is choice and protection. The Bill prohibits compulsory requirement to present the card except to receive health benefits, veterans' services and social services.

The veteran community is strongly in favour of an access card with a photograph for these purposes.

Furthermore, another key benefit was that the card would help to prevent identity fraud (nominated by 69% of people who were aware of the card).

Optional use of card

While the access card is not an identity card, a key feature of the card design is enabling card owners to use the advantages of a high integrity card for other purposes if they choose. This is one of the objects of the card and is clearly in the Act.

Removal of the cardholder's photograph from the face of the card would make the access card unusable as a primary identification document, thereby limiting the ability of consumers to choose to use the card for other identification purposes and diminishing consumer benefits.

People presently use documents and existing Australian Government cards for identification purposes in a wide range of situations. These can range from purposes requiring a high standard of proof of identity (e.g. working in the childcare, aviation or maritime industries, fertilisers and pharmaceuticals) to situations requiring a lesser standard of proof.

At present, Medicare cards are often used to support claims to a name. It is the government's position that it be up to the individual cardholder to decide if they want to show the access card. In a world where identity fraud and identity theft is a key problem, having a high quality card with a photo visible for the cardholder to use is of great utility and one that our market research suggest that people want to use as they see fit. For those people without photographic documentation, such as war veterans, the elderly and the vision impaired, the ability to voluntarily show a card with their name and photograph can be a key benefit in itself.

For example, the access card provides an opportunity for blind and low vision people to have a nationally accepted photographic form of ID, which will greatly improve the level of equity for people who are visually impaired. In testimony to the Senate Inquiry, the Blind Citizens of Australia was supportive of the access card being a good form of photographic identification.

Making a photograph on the surface of the access card optional would also create two classes of cards, only one of which could be used as a primary identification document.

To take a practical example, a card including the holder's photograph could be used as primary proof of identity in opening a bank account, ie. 70 points of value under the '100 point test'.

A card without photograph could not be used as primary proof of identity. It would be similar to the existing Medicare card which is worth only 25 points of identity.

THE NEED FOR THE CARD NUMBER ON THE SURFACE OF THE CARD

The card number is integral to the business operation of the DVA, Centrelink and Medicare Australia.

Most Australians are familiar with using card numbers over the phone to carry out different transactions. Having a convenient and easily quoted number assists customers with telephone and online transactions with participating agencies. It is always followed by a secret question and answer but the number saves considerable time.

DHS agencies undertake 51.2 million telephone contacts, 281,000 contacts via email and 74 million secured customer transactions (including Medicare) per year. The card number is essential for the speedy operation of call centres and ease of access to online services. The CEO of Centrelink has confirmed that Centrelink needs a number of the surface of the card. Medicare Australia strongly supports a photograph on the face of the card so it can be confident that people only receive benefits for Medicare and pharmaceutical services to which they are entitled.

There are hundreds and thousands of Smiths, Jones, Chans, Nguyens and Johnsons. Their transactions are made faster by being able to quote a visible number. Without a number more questions need to be asked to establish who the call centre is speaking to. The absence of a visible number would blow out waiting times for calls to be answered and increase costs to the Australian taxpayer.

If the number were not on the face of the card, there would be several disadvantages:

- People who contact agencies over the phone would be required to identify themselves by other means, using multiple references. This would be a greater intrusion of their privacy and customer interactions will be lengthier, more complicated and less convenient.

- Some customers particularly the elderly, may have difficulty remembering numbers without these being easily visible. For example, the average Veterans Affairs customer is eighty four years of age. Removing the number would disrupt services to veterans.

- In the event that the systems fail, the ability to continue processing transactions would be compromised in the absence of a visible card number.

Centrelink and Medicare see the visible card number as critical to their operations.

DVA case studies

Two of DVA's cards that are included in the access card project are the Gold and White cards. The primary purpose of these cards is the procurement of health services funded by DVA. In fact, DVA purchases close to $5 billion of services per year on behalf of the entitled members of the veteran community. The gold and white

cards are integral for this process with a reliance on the service provider quoting the number from the face of the card to raise the necessary invoice or correspondence with DVA.

DVA's gold and white cards have a secondary use with some concession providers recognising the cards and providing concessions to the cardholder. These are concessions that are not funded by the Commonwealth and it is the concession provider making a business decision to provide the service to the veteran community.

As the card is so integral to DVA business, DVA has a long standing practice of encouraging the veteran community to produce their cards and to quote their number when interacting with service providers, DVA, and to receive concessions.

DVA is opposed to the removal of the access card number from the face of the card. The majority of DVA's business is not conducted in person and therefore DVA must have a robust process to authenticate a person as quickly as possible when they make contact by phone or letter. The current practice for a DVA client to authenticate themselves is to quote the number on their card.

It is expected that as DVA cards are replaced, our clients will find it increasingly difficult to remember or find their DVA reference number. If a card number is not printed on the card the client will need to identify themselves by multiple references and will require DVA staff to search through multiple records before finding the correct client. This would make client contact more difficult and time-consuming for the customer than present arrangements. Printing the access card number on the access card will ensure consistency with current practices and maintain the convenience of being able to quote a readily available number from the face of a card.

Although most of the contact by veterans and war widows with DVA is on the telephone, veterans and war widows have very frequent personal face-to-face contact with a wide range of 50,000 contracted providers of health and community services. A large number of these occur in the home or community setting.

The introduction of the access card will require changes to business processes for service providers, however service providers may continue to manually invoice DVA during the access card transition period and will rely on the visibility of the access card number for this purpose. Further, in the event that automated systems are not functioning, the visibility of the access card number will enable continuity of business.

In addition, it is likely that many allied health providers whose clients are a combination of private (fee paying) and DVA customers (where entitlement to the service is assured on the production of their gold card) may not want any additional infrastructure for their business on the introduction of the access card in the form of any readers, let alone larger photographic readers. These small businesses are likely to want to continue to use their existing process of manually invoicing DVA and rely on the number of the face of card.

Example:

1. A gold cardholder over 80 years old no longer requires prior approval before getting a taxi to attend a medical appointment. DVA relies on the taxi driver quoting the card number from the face of the card in order to claim payment from DVA.
2. Allied health providers know that they can provide certain services to Gold cardholders. As the cardholder can be authenticated and their entitlement is verified via the colour of the card there is no need for these allied health providers to dock the card to read the entitlement status. These providers will rely on the number printed on the face of the card to invoice DVA.
3. Currently doctors wishing to prescribe certain medications are required to obtain approval from DVA. This is a telephone service where the medical practitioner phones a dedicated DVA telephone number to discuss the individual case with DVA's pharmacist, often with the patient in the consulting rooms. The current practice relies on the doctor quoting the person's card number. The access card will need to continue to support this practice.
4. Some DVA funded medical and allied health services are provided in the veteran's home. For instance, a community nurse visits a veteran in their home and records the cardholder's number on a payment voucher with the veteran confirming receipt of that service by signing the voucher. To continue to provide this service, the community nurse will need to have easy access to card number.

THE NEED FOR THE SIGNATURE ON THE SURFACE OF THE CARD

The Australian Government decided to include a digitised signature on the access card, chip and Register because it provides greater utility and security for the card owner. This is covered on page 8 (recommendation 15) of the Australian Government Response to Report 1 of the Fels Taskforce.

In his 8 November Press Club address the then Minister for Human Services, the Hon Joe Hockey MP, said that the Australian Government had decided to proceed with a digitised signature on the face of the card to make it easier to cross check signatures on the 50 million forms that are completed every year at Centrelink, Medicare and other Government offices.

The digitised signature provides greater potential for security for the card owner by enabling a visual comparison of the signature at point of service and via mail requests.

The veterans' community was particularly in strong favour of retaining the digitised signature on the surface of the card to enable the transaction of their unique benefits.

DVA Case Studies

DVA gold and white cards are Commonwealth funded procurement cards and have the cardholder's signature on the back of the card. Given that most of the contact by veterans and war widows with DVA is not face-to-face, the signature is currently the

primary means of authentication for DVA's service providers. Without this means of authentication, DVA has little or no recourse for fraud purposes. Upon the introduction of the access card, the signature will be used by service providers as a secondary means of authentication when a veteran or war widow signs the form confirming receipt of the service.

Without a photograph and signature on the card, the service provider will have to dock the access card or contact DVA to verify that the individual is in fact the rightful cardholder and entitled to receive the service (e.g. medication administration). It goes without saying that there are major mutual benefits with these features for all frail, confused or demented clients.

As outlined above, there are a number of circumstances where the service provider will not have an access card reader or generally has no need to check entitlement status as it is apparent due to the colour of the card produced.

DOCUMENT VERIFICATION – WHY WE ARE NOT RELIANT ON THE DOCUMENT VERIFICATION SERVICE (DVS)

Verification of documents is not dependent on any single system. The following systems will be used:

- The existing National Exchange of Vehicle and Driver Information System (NEVDIS) for state and territory issued driver's licenses. From April 2008 we will be able to verify all drivers' licences with the exception of Tasmania, which is planned to come on board later in 2008. NEVDIS is also used in an online mode by the Department of Immigration and Citizenship.

- The existing Certificate Validation Service (CVS) for electronic verification of birth certificates. The CVS commenced operation in 2000 and currently covers NSW, Victoria, Western Australia, South Australia and the ACT. Queensland, the Northern Territory and Tasmania are expected to join mid this year, that is, before commencement of access card registration.

- The Document Verification Service, where it is available. At this stage it is anticipated to be available for Department of Foreign Affairs and the Department of Immigration and Citizenship issued documents such as passports, visas and citizenship certificates.

- Manual verification can is also an option where electronic data is not available.

SECURITY AGENCIES WILL NOT HAVE UNFETTERED ACCESS TO THE REGISTER

During proceedings on 6 March, a series of question was put to Mr Paul O'Sullivan, Director-General of Security by Senator Nettle which related to the access which ASIO might have to information on the access card Register.

At one point Senator Nettle referred specifically to my earlier answers in Senate Estimates. My answer was a verbatim quote of material from the Australian Government Solicitor. I have discussed this matter with Mr O'Sullivan and our Legal Counsel have conferred. ASIO does not disagree with the statements I made at Senate Estimates as set out in the Hansard.

To confirm, ASIO may ask DHS for information from the access card Register. DHS has the discretion to give or not give that information to ASIO. If DHS does not give that information to ASIO, ASIO can only compel DHS to give that information to it in accordance with a search warrant issued pursuant to the *ASIO Act 1979*.

The Director-General of Security has already outlined this morning the significant safeguards and accountability mechanisms to which ASIO is subject.

Attachment 1

Examples of social services access cards in other countries

With ongoing pressure on government budgets around the world and growing concern about identity theft, there is considerable focus on ensuring only eligible citizens receive government benefits and services and only those benefits and services to which they are entitled:

- Europe's two biggest democracies, France and Germany, between them accounting for about 130 million citizens, have decided that in order to reduce fraud it was necessary to upgrade the integrity of their existing health chip-cards by including a photograph on the face of the card.
- Various countries, such as Taiwan, have claimed significant fraud savings from requiring a smartcard displaying a photograph to access health and social benefits.
- Other countries where a photo has not been included on their social services cards have a photo-based national ID card to accompany the social services card (e.g. Italy and Belgium).

It is also commonplace around the world to require photo-based cards in order to access concessional benefits such as concessional travel. For instance, in the UK and Singapore, transit cards are generally anonymous with no photo but a photo is required on the card in order to claim concessional travel benefits. The proposed Victorian smartcard "myki" will require a "personalised" card, likely displaying a photograph in order to claim concessional travel. The Victoria Government website states that applicants are to hand in two photographs when applying for their concession smartcard.

International examples are summarised in the following sections.

1) France - Carte Vitale 2

In May 2004, former Health Minister Philippe Douste-Blazy acknowledged that **there were 58 million cards for an eligible population of 48 million people**, which according to him provided evidence that the system was "not managed".

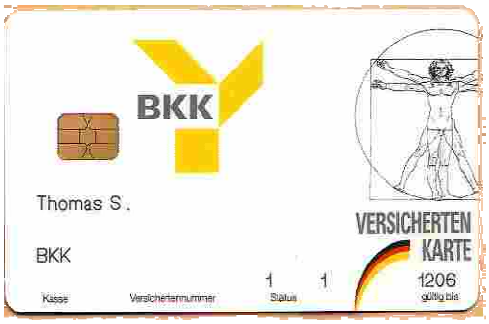
The existing health care card, Vitale 1, did <u>not</u> have a photo printed on the face of the card. The new card (Vitale 2) will contain a photo both on the face of the card and in the chip. The reason for including the photo is to combat fraud and to ensure that the person who claims the benefits is entitled to them.

Old card ***New card***

2) Germany - Gesundheitskarte

The current German health smartcard, Krankenversichertenkarte does not contain a photo. The new card, Gesundheitskarte, will contain a photo on the face of the card but not in the chip. The reason for including the photo is to combat fraud.

Current card ***New card***



In fact, to combat fraud, some national insurance companies in Germany like the AOK Baden Württemberg have already placed a photo on the current Krankenversichertenkarte and have positive results in terms of less fraud and a much reduced loss rate ("customers take better care of the card"). Feedback from the medical community on the addition of the photo is also positive.

Fraud estimates for the current system in Germany run at between 800 million and 2 billion Euro (about A$1.3 to 3.2 billion) in fraud annually. The current non-photo chip-cards are reported to be worth between 50-200 euros on the black market.

3) Taiwan – Health card

Taiwan introduced the Health card for access to health services from 2002. This was the first such card in Taiwan. The card displays a photo which was scanned from documents.

The Bureau of National Health Insurance has stated that "In the first year of implementation, we also believe we can reduce various fraud claims, thus saving us a further US$210 million".

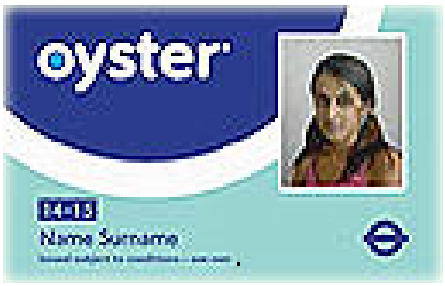
Travel concession cards

1) Victoria - 'Myki' Transport Card

The Victorian transport card it will be possible to personalise a myki with a name and/or a photo. For concession myki, holders will be required to have a personalised myki.

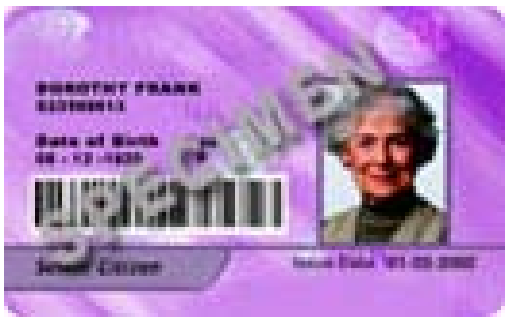
2) London – Oyster card

Oyster cards with a photo are issued to holders that are eligible for free or concessional travel.



3) Singapore – ez-link cards

Ez-link cards with photos are issued to holders that are eligible for concessional travel.



Attachment 2

Card Reader Types

Basic Reader – Single Line Display

This low cost device is an 'envelope-style' reader approximately the same size as the card – the card slips into the reader – and is designed to be carried in the purse or pocket. Has only a single line display to show concessional status.

Without a photo on the surface of the card, fraud is not stopped – people can pretend to be someone else.

Basic Reader – Single Line Display

This low cost device has no thumbwheel but has two function keys on the right that could be used as Scroll Up and Scroll Down keys if required.

Battery life up to 20,000 card insertions depending upon card type and application.

Has only a single line display to show concessional status.

Without a photo on the surface of the card, fraud is not stopped – people can pretend to be someone else.

Basic Reader with Thumb Wheel

This low cost device is the same as the one above, but does not include a numeric keyboard. Instead, it has a circular thumbwheel on the right side which may be used to scroll up or down through displayed data.

Without a photo on the surface of the card, fraud is not stopped – people can pretend to be someone else.

Point of Sale Terminal

This high cost device contains, PIN pads, generally include a magnetic stripe reader, an EMV compliant contact chip reader, a backlit graphics display and a secure numeric keyboard plus three or four programmable function keys. This device is not designed to display a photo and will only show a limited number of text fields.

Without a photo on the surface of the card, fraud is not stopped – people can pretend to be someone else.

Point of Sale Photo Capable Terminal

This is a very high cost unit. Several manufacturers do offer POS terminals capable of displaying a photograph. Examples include the Hypercom Optimum L4100 terminal (see the discussion of reader types at Attachment 2), Verifone MX870 and the Ingenico I6700. These are high end POS terminals and have been used by some US retailers to display advertising or coupons. Generally, the terminal

faces the consumer and can not be easily seen by the healthcare provider or retail clerk.

Terminals in agencies

Terminals in agencies will be linked to the customer service officer's computer and the photo will be displayed on the monitor.