Australian Government

Department of Broadband,
Communications and the Digital Economy

Regulation Impact Statement

Proposed Changes to Identity Verification Requirements for Prepaid Mobile Services

February 2013

1. Background

Prepaid mobile services have historically been viewed as a popular option for users with low usage requirements and basic or inexpensive handsets. Due to the way in which they are paid for, prepaid services allow people to better control their spending, and are suitable for people who would not be able to pass the credit checks required for post-paid accounts. They can also alleviate the risk of debt in some demographics, particularly teenagers, who have the potential to incur excessive mobile service bills.

More recently, prepaid services have expanded to encompass a wider range of products, such as tablets, computers and wireless dongles, and are amongst services increasingly being used as an alternative to international roaming.

Prepaid mobile service providers are required by law to collect certain information about their customers and to verify their customers' identities before activating a service. The requirements have been put in place to prevent the use of anonymous prepaid services and ensure that law enforcement and security agencies can gain accurate information about prepaid customers should they need to do so as part of their investigations. The information collected can be disclosed to law enforcement and security agencies upon lawful request in accordance with legislation such as the *Telecommunications Act 1997* and the *Telecommunications (Interception and Access) Act 1979*. The requirements support the obligation of service providers under section 313 of the *Telecommunications Act 1997* to prevent their networks or facilities from being used to facilitate the commission of offences.

The current requirements are specified in the *Telecommunications (Service Provider – Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000*, made by the Australian Communications and Media Authority (ACMA). This Determination is made in accordance with the *Telecommunications Regulations 2001*. Under the Determination, the retailer selling a prepaid SIM sights one or more commonly held "Category A" or "Category B" identity documents as detailed in the Determination and completes a form as part of the sale. The retailer then sends the completed form to the service provider for its records and storage. The consumer activates the service through a separate process at which time he/she provides certain information again, such as name and address. The information from this second process is placed in the Integrated Public Number Database[1] and the service provider's records.

When the current identity verification requirements were first introduced in 1997, the Determinations under which they were made were relatively open as to how and when the verification process was to occur; carriers and carriage service providers were simply required to verify the customer's identity prior to activating the service.

The ACMA then amended the arrangements in 2000 to set out explicit obligations for the verification process at the point of sale. It also amended the regime to introduce an alternative

[1] The Integrated Public Number Database is a centralised database of all Australian telephone numbers and associated subscriber information. The database provides information to support a range of services, including the Triple Zero emergency call service, the dissemination of telephone-based emergency warnings and investigations by law enforcement and security agencies.

mechanism to allow verification to occur at the point of activation. Despite the introduction of this new mechanism, however, point of sale verifications continued. Adoption of the point of activation method was low and proved difficult to implement, since there were no identifiable mechanisms with which a service provider could verify a customer's identity online or over the phone with confidence.

In 2004, the ACMA further amended the Determination to introduce a third option for identity verification, in which a service provider could submit an alternative model for compliance. While there has been some discussion regarding the use of this third option, no suitable alternative has ever been approved by the ACMA.

The ACMA reviewed the arrangements in 2006, with the aim of introducing improvements to processes to address the concerns of law enforcement and security agencies. As recommended by the review, industry and the Australian Mobile Telecommunications Association (AMTA) developed and deployed a new common point of sale form in 2008 in addition to ongoing awareness campaigns.

The ACMA undertook two compliance audits following the review. The first audit, conducted prior to the introduction of the improvements, found compliance levels to be poor. The second audit was conducted shortly after the introduction of the form and while it showed improvement, compliance levels remained a concern.

1.1. Prepaid mobile market

There are an estimated 30.2 million mobile voice and data services in operation in Australia, with 39 per cent (11.6 million) being prepaid and 61 per cent (18.6 million) being post-paid.[2]

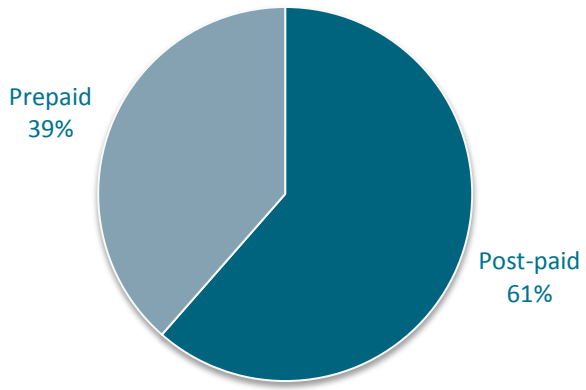
Table 1: Total mobile voice and data services in operation

Year	Post-paid no. (mil)	Post-paid %	Prepaid no. (mil)	Prepaid %	Total no. (mil)	Total %
2009-10	15.28	59%	10.71	41%	25.99	100%
2010-11	18.05	62%	11.23	38%	29.28	100%
2011-12	18.56	61%	11.64	39%	30.20	100%

Source: ACMA Communications Report 2011-12, p.32

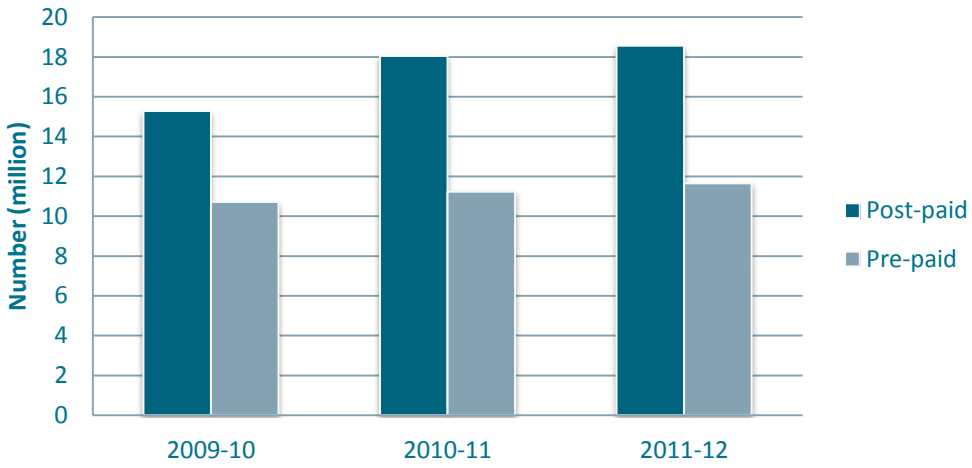
[2] ACMA, *ACMA Communications Report 2011-12*, p.32 http://www.acma.gov.au/webwr/_assets/main/lib550049/comms_report_2011-12.pdf; figures include wholesale and retail services and wireless broadband data services provided via data cards, dongles or USB modems.

Chart 1: Percentage of total prepaid and post-paid mobile voice and data services 2011-12



Source: ACMA Communications Report 2011-12, p.32

Chart 2: Prepaid and post-paid mobile voice and data services 2009-10 to 2011-12



Source: ACMA Communications Report 2011-12, p.32

There are three mobile network operators in Australia: Telstra, Optus and Vodafone Hutchinson Australia (VHA). Telstra sells mobile services under its own brand, Optus sells under its own brand as well as its subsidiary, Virgin Mobile, while VHA operates the Vodafone, 3 and Crazy John's brands. The network operators also lease network capacity to Mobile Virtual Network Operators (MVNOs) who sell mobile services under separate brands, usually to targeted segments of the market. The MVNO market is relatively dynamic, with operators able to easily

enter and leave the market. Based on information provided by the mobile network operators in 2011, there are approximately 20 major MVNOs that sell prepaid services. In addition to the mobile network operators and MVNOs, prepaid SIMs are sold by an estimated 30 000 third party retailers,[3] including supermarkets, convenience stores, electronics stores and mobile phone resellers.

While each mobile network operator uses different terminology in their reports, similar data indicates that approximately a third of Telstra[4] (33 per cent) and VHA's[5] (36 per cent) mobile services, and 44 per cent of Optus'[6] mobile services are prepaid. These figures indicate that Optus has the largest share of the prepaid mobile market, followed by Telstra and VHA.[7]

Table 2: Mobile services operated by the three mobile network operators 2011-12[8]

Carrier	Post-paid no. (mil)	Post-paid %	Prepaid no. (mil)	Prepaid %	Total no. (mil)	Post-paid market share	Prepaid market share
Telstra	6.596	67%	3.267	33%	9.863	41%	33%
Optus	5.285	56%	4.227	44%	9.512	33%	42%
VHA	4.360	64%	2.484	36%	6.844	27%	25%
Total	**16.241**	**62%**	**9.978**	**38%**	**26.219**	**100%**	**100%**

Source: company annual reports, 2012

[3] Paragraph 2.4.9, AMTA submission, *Productivity Commission's Annual Review on Regulatory Burdens*, February 2009, http://www.pc.gov.au/__data/assets/pdf_file/0019/86302/sub005.pdf

[4] Telstra, *Telstra 2012 Annual Report*, p.20, http://www.telstra.com.au/abouttelstra/download/document/Telstra-Annual-Report-2012.pdf; using the number of post-paid and prepaid handheld retail mobiles

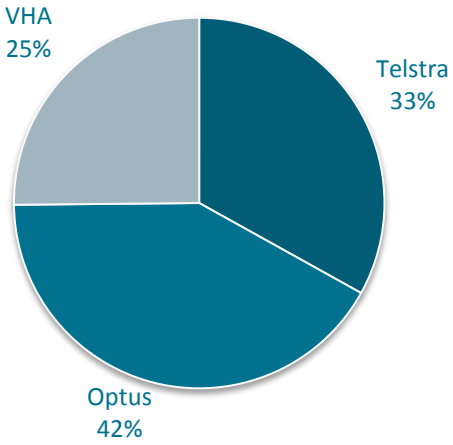
[5] Hutchison Telecommunications (Australia) Limited, *ASX Half Year Information,* 30 June 2012, p.8, http://clients.weblink.com.au/clients/Hutchison2/article.asp?view=2686909; using the number of mobile customers, excluding customers of MVNOs

[6] Singapore Telecommunications Limited and Subsidiary Companies, *Management Discussion and Analysis of Financial Condition, Results of Operations and Cash Flows for the Second Quarter and Half Year Ended 30 September 2012*, p.44, http://www.optus.com.au/dafiles/OCA/AboutOptus/MediaCentre/SharedStaticFiles/SharedDocuments/Q2FY13_MDA.pdf; using the number of post-paid and prepaid mobile subscribers

[7] Company annual reports 2012, as above.

[8] Refer to footnotes regarding figures from company reports above.

Chart 3: Prepaid mobile market share by mobile network operator 2011-12



Source: company annual reports, 2012

Telstra reported revenue of $654 million from prepaid mobiles for 2011-12, an increase of 2.7 per cent from the previous year.[9] Optus and VHA do not report on total revenue from their prepaid mobiles sales. Based on market shares, it is estimated that total revenue from prepaid mobiles is likely to be in the order of $2 billion per year for the three network operators.[10]

For the half year ended June 2012, Telstra reported an average revenue per user of $16.67 per month for prepaid services (compared to $63.69 per month for post-paid services),[11] while for the quarter ended June 2012, Optus reported $21 for prepaid services (compared to $60 for post-paid services).[12] VHA does not provide a split of revenue by prepaid and post-paid.

While there are only three mobile network operators, there are a range of factors that promote competition in the domestic prepaid market, including:

- the low cost to entry (a SIM generally costs $2 and there are no credit checks)
- the absence of contracts (customers are not locked-in for long periods of time)

[9] Telstra, *Telstra 2012 Annual Report*, p.15 http://www.telstra.com.au/abouttelstra/download/document/Telstra-Annual-Report-2012.pdf

[10] Based on Telstra's total prepaid revenue and Optus' average revenue per user, and assuming that VHA's average revenue per user is of a similar magnitude.

[11] Telstra, *Telstra 2012 Annual Report*, p.20, post-paid figure excludes Mobile Repayment Option http://www.telstra.com.au/abouttelstra/download/document/Telstra-Annual-Report-2012.pdf

[12] Singapore Telecommunications Limited and Subsidiary Companies, *Management Discussion and Analysis of Financial Condition, Results of Operations and Cash Flows for the Second Quarter and Half Year Ended 30 September 2012*, p.44 http://www.optus.com.au/dafiles/OCA/AboutOptus/MediaCentre/SharedStaticFiles/SharedDocuments/Q2FY13_MDA.pdf

- the ease and low cost of shifting to another service
- the low cost for customers to simultaneously hold multiple services from one or more providers
- homogenous products and national pricing, while recognising that there are some differences in network coverage and performance
- regulations regarding advertising that assist consumers in comparing services
- mobile number portability, which allows a customer to quickly, easily, and without charge transfer their mobile number to a new service with the same or another service provider
- MVNOs that actively target certain segments of the market and seek to differentiate themselves from the three network operators, for example by offering different plans.

The churn rate for prepaid mobile services (both within a provider and between providers) is understood to be considerably higher than that for post-paid services, suggesting the dynamic nature of the market and the low barriers for consumers to seek the most competitive service.

2. Problem

A number of changes have significantly reduced the effectiveness and efficiency of the current identity verification requirements.

When the availability of prepaid SIMs was limited to service provider shopfronts, service providers were the only entities required to verify the identity of their customers. The current requirements were created with this centrally-focused business model in mind. However, information from industry[13] and the ACMA points to significant growth in the number of third party retailers selling SIM cards, with AMTA estimating that there are some 30 000 third party retailers.[14] This means that a greater range of entities are now required to verify the identity of prepaid mobile customers on behalf of the service providers.

Further, as business models shift to take advantage of the internet, the number of service providers and third party retailers integrating online activities into their business practices is increasing. Telstra, for example, has reported that its online transactions grew from approximately 22 per cent in 2011[15] to 30 per cent in 2012[16], and that it has a target of 35 per

[13] *Australian Mobile Telecommunications Industry Economic Significance, Report to the Australian Mobile Telecommunications Association*, the Allen Consulting Group, September 2005, p.14; http://www.amta.org.au/files/state.of.industry.report.2005.pdf

[14] Paragraph 2.4.9, AMTA submission, *Productivity Commission's Annual Review on Regulatory Burdens,* February 2009, http://www.pc.gov.au/__data/assets/pdf_file/0019/86302/sub005.pdf

[15] Telstra, *Telstra Sustainability Report 2011*, p.19, http://telstra.com.au/abouttelstra/download/document/2011-sustainability-report.pdf

[16] Telstra, *Telstra 2012 Annual Report*, p.xi, http://www.telstra.com.au/abouttelstra/download/document/Telstra-Annual-Report-2012.pdf

cent of transactions being online by the end of 2012/13.[17] In such cases, it becomes difficult to verify the identity of the customer purchasing the service through the existing identity verification arrangements, which were designed to be carried out face-to-face and are predominately paper-based.

The telecommunications industry and law enforcement and security agencies have voiced longstanding concerns with the current requirements.

Industry's concerns include:

- The high cost of the current requirements, including identity checks, paper-based personal information forms and storage (estimated by AMTA in 2009 to be $10 million per year ($11 million adjusted for inflation))[18].
- Liability for non-compliance rests with the service provider. Service providers state that they have little scope for enforcement action against third party retailers. As identity checks are completed at the point of sale by a large number of retailers, it is therefore difficult to ensure compliance.
- Third party retailers' reluctance to continue with identity checks.
- There is difficulty for some customers, such as minors, to satisfy the identity checks.

Concerns for law enforcement and security agencies include:

- The difficulty of retrieving identity information when required due to the use of a paper-based system. Agencies argue that the lack of reference to storage and retrieval requirements in the Determination has resulted in industry implementing a least cost solution that does not support the timely retrieval of information.
- Identity checks can be relatively easily circumvented through identity fraud due to difficulties in validating identity documents by retail sales staff.
- The system does not offer retailers clear incentives to comply.

Other concerns include:

- Consumers must provide the same personal information both at the point of sale and again at the point of activation.
- Consumers may be asked to provide personal details and evidence of identity in a retail environment in which they may not have confidence that their privacy and information will be appropriately safeguarded.

[17] Telstra, *Telstra Sustainability Report 2011*, p.19, http://telstra.com.au/abouttelstra/download/document/2011-sustainability-report.pdf

[18] Paragraph 2.4.3, AMTA submission, *Productivity Commission's Annual Review on Regulatory Burdens,* February 2009 (submission date), http://www.pc.gov.au/__data/assets/pdf_file/0019/86302/sub005.pdf

- There are other difficulties in identifying the end users of prepaid SIMs because:
  - purchasers of prepaid services may lend or give them away
  - around 150 000 mobile devices are reported lost or stolen each year to AMTA, with about 50 000 of these being later reported found[19]
  - the entire Australian regime can be avoided by importing prepaid services from overseas.

The telecommunications industry raised its concerns in a submission to the Productivity Commission's 2009 Annual Review of Regulatory Burdens on Business. In response, the Productivity Commission recommended that:

> *The Australian Government should review the costs and benefits of identity checks for prepaid mobile phone services in consultation with law enforcement and security agencies. The review should have the objective of substantially revising the regime to better achieve its objectives while eliminating unnecessary costs to business.* [20]

Additionally, the Parliamentary Joint Committee on the Australian Crime Commission has stated that "the current requirements for recording SIM card user details are deficient and therefore represent a significant difficulty to authorities needing to accurately track suspect mobile phone users. This is a critical area needing urgent attention"[21].

In order to address the concerns identified by stakeholders and to investigate ways that industry can better meet its regulatory obligations, the department led a first-principles review of identity verification requirements for prepaid mobile service customers. In 2009, it established a Prepaid Working Group comprising representatives of the Attorney-General's Department (AGD), the ACMA, AMTA, the Office of the Australian Information Commissioner, the Australian Federal Police, Telstra, Optus and Vodafone Hutchison Australia. The working group was established under the auspices of the Commonwealth and Industry Telecommunications Experts Group co-chaired by the department and AGD.

This working group sought to develop a solution which addresses the concerns raised by stakeholders using the objectives provided below.

3. Objectives

The objective of the proposed changes is to address the problems outlined above, and create a solution that:

---

[19] AMTA, *Lost and Stolen Phones,* http://www.amta.org.au/pages/Lost.and.stolen.phones (as at 18 February 2013)

[20] Recommendation 4.3, Productivity Commission, *Annual Review of Regulatory Burdens on Business: Social and Economic Infrastructure Services*, August 2009, http://www.pc.gov.au/projects/study/regulatoryburdens/social-economic-infrastructure/report

[21] Parliamentary Joint Committee on the Australian Crime Commission, *Executive Summary,* September 2007, http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=acc_ctte/completed_inquiries/2004-07/organised_crime/report/b01.htm (as at 18 February 2013)

1. is practical, effective and cost efficient
2. is flexible to support current and future business models
3. enables the 99 per cent of prepaid customers who wish to activate their service online or over the phone to do so
4. improves on the information privacy standards of the current method
5. improves service provider compliance with the Determination
6. improves on the inefficiency of the paper-based system for law enforcement agencies
7. removes duplication of the provision of information at both point of sale and point of activation.

4. Options

Informed by the outputs of the working group, the department has identified the following options as potential solutions to achieve the above objectives:

1. Retain the status quo.
2. Remove the requirements for identity verification.
3. Improve the existing method where a customer's identity is verified at the point of sale.
4. a) Replace the existing method where a customer's identity is verified at the point of sale with new methods at the point of activation.

   b) Allow service providers to use identity verification methods at the point of activation, as well as the existing method.

Option 1: Retain the status quo

Under this option, no changes would be made to the existing identity verification methods. Verification would continue to occur at the point of sale and users would provide their information again at the point of activation.

Option 2: Remove the requirement for identity verification

Under this option, service providers would not be required to verify the identities of their prepaid mobile customers.

Option 3: Improve the existing method where a customer's identity is verified at the point of sale

Under this option, customers would continue to verify their identity at the point of sale and provide their information again at the point of activation, though in a revised form or using new methods.

The Prepaid Working Group considered this option and concluded that there were no viable improvements that could be made which addressed the concerns identified by stakeholders.

Option 4a: Replace the existing method where a customer's identity is verified at the point of sale with new methods at the point of activation

This option was proposed by the Prepaid Working Group and endorsed by the Experts Group.

Under this option, the current method where a customer's identity is verified at the point of sale would be removed by a certain date and service providers would be required to verify a customer's identity when activating the service using one of the following new methods:

- transferring a small sum to the customer's bank account to verify its existence
- verifying the details and validity of a government-issued document using the National Document Verification Service (DVS) or Visa Entitlement Verification Online (VEVO)
- verifying a 'trusted' email address ending in either ".edu.au" or ".gov.au"
- delivering the SIM card via signed and receipted courier delivery
- verifying a customer's existing post-paid account.

Service providers would also be able to verify a customer's identity if the customer uses a credit card or EFTPOS card for a transaction that the service provider is party to. This is because the service provider in this case will have details of the financial transaction. In addition, a service provider will be able to verify a customer's identity by sighting the customer's identification at the service provider's shopfront, which is somewhat similar to the current arrangements. It is proposed to maintain the option to sight a customer's identity documents as some customers may be unable or choose not to verify their identity online or over the phone using one of the specified methods. However, this will only be possible at a service provider's shopfront where the provider is able to activate the service – not at a shopfront of a third party retailer – and is envisaged to only apply to a small number of customers.

The methods will allow verification to occur online, over the phone or at a service provider's shopfront. The proposal means that a customer will be able to purchase a prepaid service without having to provide any evidence of identity at the point of sale, making the sale a regular retail transaction.

A key method proposed for identity verification will be use of the DVS. This service is managed by AGD and is a national, real-time, online document verification system. It provides a single entry point to verify and validate a range of Commonwealth and state and territory identity documents with the issuer of the document. A customer would provide (or enter online) identifying information for government-issued documents that would be sent in real time to the DVS, which would verify with the issuing agency whether the information is correct and provide a rejection message if the information does not match the agency's records. For example, a passport number and a person's name and date of birth included on a passport would be verified with the Department of Foreign Affairs and Trade.

As part of the 2012-13 Budget, the government announced that it will extend access to the DVS to the private sector from 2013-14 to assist businesses in meeting their identity verification requirements.

It is proposed that the private sector will be able to verify the following documents using the DVS:

<u>Commonwealth government documents</u>

- Medicare cards
- passports
- visas

- citizenship certificates

State and territory government documents (subject to state and territory agreement)

- driver's licences
- learner's permits
- birth certificates
- marriage certificates
- change of name certificates.

Service providers will only be required to record the type of document or verification method, the customer's identity information (such as name and date of birth) and the outcome of the verification, not the identifying number of the document (such as passport or driver's licence number).

It is proposed that only one form of identity verification method will be required, replacing the current requirement to produce a certain number of "Category A" and "Category B" documents as outlined in the Determination. However, as referred to above, if a customer is unable to or chooses not to verify his or her identity online or over the phone using one of the specified methods, he or she can still produce identity documents at the service provider's shopfront similar to existing requirements. Special arrangements will be made for people who do not have the required evidence of identity, such as people in remote and indigenous communities and people who have lost their identity documents as a result of a natural disaster.

Under the proposal, service providers would also be required to collect a customer's date of birth. This is to assist law enforcement and security agencies in accurately identifying customers, particularly those with the same name.

This proposal would require service providers to replace the existing point of sale identity verification method with the new identity verification methods at the point of activation by a certain date.

The Appendix contains two diagrams, one outlining the identity verification process using the DVS and VEVO (**Diagram 1**), and another illustrating the flow of information in a DVS transaction (**Diagram 2**).

Option 4b: Allow service providers to use identity verification methods at the point of activation, as well as the existing method

Under this option, the proposed new identity verification methods from Option 4a would be run in parallel with the existing methods, and service providers would have the flexibility to choose between the current verification method or adopt new methods as they became available. Unlike Option 4a, there would be no hard cut-over, and service providers would be able to adopt verification methods according to their business requirements. Consideration would be given to removing the existing point of sale method after a period of time (see "Implementation and review" below).

5. Impact analysis

Below is an analysis of the costs and benefits of each of the proposed options as compared to the status quo. The analysis covers the costs and benefits to consumers and the general

community, law enforcement and security agencies, industry (service providers and third party retailers) and the ACMA.

5.1. Option 1: Retain the status quo

5.1.1. Costs

If the existing method for identity verification remains in place, the issues identified by industry, law enforcement and security agencies, and consumers will persist.

The running costs of the current identity verification requirements would continue in their present form. In 2009, AMTA estimated the cost of the current identity verification requirements to the telecommunications industry as approximately $10 million per year[22], which is estimated to be $11 million adjusted for inflation. However, when factoring in the 30 000 third party retailers and their role in the verification process, AMTA estimated that this cost increases to approximately $26-$27 million ($29-$30 million adjusted for inflation). This equates to $5.70 per SIM ($6.25 adjusted for inflation).

Under section 314 of the *Telecommunications Act 1997*, mobile service providers can recover the cost of providing assistance to law enforcement and security agencies; however, this does not cover the cost associated with implementing the regulatory requirements.

If the status quo were to be retained, the inefficiencies resulting from verifying a customer's identity using primarily paper-based methods – where the trend is for businesses to move their practices online – will persist. This means that it is likely to become more difficult for retailers and service providers to comply with the requirements.

5.1.2. Benefits

In its submission to the Productivity Commission's 2009 Annual Review of Regulatory Burdens on Business: Social and Economic Infrastructure Services, AGD stated that:

> *The information gathered under the Determination has been vital to investigations of terrorists, murderers, drug traffickers, kidnappers and those who have committed crimes of violence.*
>
> *Without accurate purchaser information, investigations by law enforcement and national security agencies could be significantly hindered. It is common practice for individuals seeking to avoid scrutiny from security or law enforcement agencies to try to avoid using properly subscribed prepaid mobile telecommunications services. The*

[22] Paragraph 2.4.3, AMTA submission, *Productivity Commission's Annual Review on Regulatory Burdens,* February 2009, http://www.pc.gov.au/__data/assets/pdf_file/0019/86302/sub005.pdf

abolition of this policy would allow all persons of interests to purchase mobile devices anonymously, thereby avoiding lawful interception of their communications.[23]

In addition to the benefits to law enforcement and national security, service providers would not need to implement any new arrangements if the status quo were maintained.

5.2. Option 2: Remove the requirement for identity verification

5.2.1. Costs

As previously discussed, identity verification for prepaid mobile customers is an effective tool for law enforcement and security agencies, as the information collected by service providers assists their investigations of persons of interest. AGD has stated that "the abolition of the requirement that identity checks be made for pre-paid mobile telecommunications would result in a serious reduction in the capability of law enforcement agencies and therefore cannot be supported."[24] The information is also used by the Integrated Public Number Database, which is used for critical services such as the Triple Zero emergency call service and the emergency alert system.

In March 2006, the ACMA released a discussion paper entitled "*Improving Identity Check Processes for Pre-paid Mobile Services*".[25] Submissions to this discussion paper argued that there is little or no commercial need for prepaid mobile service providers to obtain, verify and retain identity and address information about customers.

5.2.2. Benefits

Removing the requirements would free industry of the compliance costs as estimated above. Further, the ACMA would also experience savings from not enforcing or monitoring compliance.

Prepaid mobile customers would also experience benefits if the requirement for identity verification were removed. They would save time in not having to verify their identity, and they would not have to provide personal information.

5.3. Option 3: Improve the existing method where a customer's identity is verified at the point of sale

Under this option, changes would be made to the existing arrangements where service providers and third party retailers verify a customer's identity at the point of sale, and customers provide information a second time when activating a service. Potential changes include further

[23] Submission by the Attorney-General's Department to the Productivity Commission's 2009 *Annual Review of Regulatory Burdens on Business: Social and Economic Infrastructure Services*, http://www.pc.gov.au/__data/assets/pdf_file/0008/90836/subdr086.pdf

[24] Submission by the Attorney-General's Department to the Productivity Commission's 2009 *Annual Review of Regulatory Burdens on Business: Social and Economic Infrastructure Services*, http://www.pc.gov.au/__data/assets/pdf_file/0008/90836/subdr086.pdf

[25] ACMA, *Improving Identity Check Processes for Pre-paid Mobile Services*, March 2006, p.6, http://www.acma.gov.au/webwr/_assets/main/lib100285/id_checks_prepaid.pdf (as viewed on 18 February 2013)

amendments to the point of sale form, greater use of electronic systems, and changes to procedures. However, the working group determined there were no viable improvements that could be made for the reasons outlined below.

5.3.1. Costs

A number of changes have been made to the point of sale arrangements in the past (refer to 'Background' above). Although these have resulted in some improvements, the working group determined that any further changes would not address the underlying problems inherent with the two-stage process (where identity verification occurs at the point of sale, and activation occurs through a separate process). In particular:

- some 30,000 third party retailers would continue to bear costs associated with identity verification
- the risk of non-compliance by third party retailers would remain as they would continue to verify the identities of customers on behalf of service providers
- consumers would continue to provide personal information twice – once at the point of sale, and again when activating the service
- consumers would continue to provide personal information in a retail environment and may not have confidence that their privacy will be appropriately safeguarded
- duplication between the point of sale and point of activation processes would remain.

5.3.2. Benefits

The primary advantage of this option would be that the changes build on known arrangements. This would likely make it easier for service providers, third party retailers and consumers to adapt to any changes. Depending on the nature of any changes, there could also be efficiencies to be gained from the greater use of electronic systems and a revised form and procedures.

5.4. Option 4a: Replace the existing method where a customer's identity is verified at the point of sale with new methods at the point of activation

5.4.1. Costs

There are a number of verification methods available under this option, as described under the 'Options' section. These methods include using the DVS to verify information about government-issued documents, and also other methods such as verification of a financial institution account or use of a 'trusted' email address.

There is no data available to quantify the cost of methods which do not use the DVS. However, given the expected cost components for service providers of each method (**Table 1**, Appendix) and the proposed prices for the DVS, it is estimated that the most expensive method under Option 4a would be when a service provider representative uses the DVS to verify a customer's identity documentation over the phone or at one of its shopfronts. This is because in addition to the actual DVS transaction cost, the added costs associated with labour also require consideration. The second most expensive method is expected to be where a customer verifies his/her identity using the DVS through a service provider's website (i.e. self-service).

AGD has proposed two pricing models (which are subject to further negotiations with the states and territories) for DVS verifications:

- 'Casual Rate': a tiered schedule of transaction fees which varies depending on the number of transactions made in one calendar month
- 'Subscriber Rate': a discounted tiered model where the user pays an annual subscription fee

These transaction fees are outlined in full in **Table 2** of the Appendix.

In addition to these fees, it has also proposed application and connection fees. These fees apply regardless of the type of business accessing the DVS, be it a carrier, carriage service provider, or MVNO, and are explained in the table below.

There are two main ways that a service provider may connect to the DVS. It may connect to the DVS directly using its own infrastructure, or it may use an intermediary service to facilitate its DVS transactions. Depending on this access configuration, the fees that each is required to pay will differ as outlined in **Table 3** below.

Table 3: Proposed DVS access costs

	One-off costs		**Recurring costs**	
Entity / Connection type	Application fee	Connection fee	Transaction costs (under Casual Rate)	Recurring costs (under Subscriber Rate)
Service provider – direct connection	$15 800	$84 000	$1.00 - $1.75 per DVS verification (varies depending on volume)	$0.90 - $1.65 per DVS verification (varies depending on volume) plus $200 000 (annual subscription fee)
Service provider – through intermediary	$15 800	*Determined by intermediary*	*Determined by intermediary*	*Determined by intermediary*
Intermediary service	$15 800	$84 000	$1.00 - $1.75 per DVS verification (varies depending on volume)	$0.90 - $1.65 per DVS verification (varies depending on volume) plus $200 000 (Annual subscription fee)

Use of an intermediary service will allow service providers (especially smaller ones) to take advantage of volume discounts which they would not ordinarily be able to receive if they connected directly to the DVS.

AGD advises that the DVS prices and fees will be reviewed annually and may decrease as the volume throughput increases.

The following table compares the estimated recurring verification costs using the DVS with the existing method. There will also be implementation costs (refer to **Table 1** of the Appendix for the expected cost components).

Table 4: Comparison of estimated recurring identity verification costs for service providers per SIM

Stage	Existing method	New method – DVS online (customer self-service)	New method – DVS over the phone or at service provider shopfront
Point of Sale	$6.25[26]	NIL	NIL
Activation	NIL	$1.75 (DVS)	$0.40 (Labour) $1.75 (DVS)
Total	**$6.25**	**$1.75**	**$2.15**

This information was calculated under the following assumptions:

- Only one DVS transaction is required to verify a customer's identity.
- The DVS cost calculation uses the maximum DVS transaction price ($1.75).
- The labour cost is calculated using the Australian Call Centres Award wage[27] and the Australian Telecommunications Services Award wage.[28] It also assumes an approximated on-costs value of 30 per cent of the wage rate, and a 38 hour work week.
- The section of time relevant to the identity verification process is the additional time taken to collect information about the customer's identity document that is not already collected by the service provider when activating the service, and the time taken to check its validity with the DVS.[29] This is estimated to take no longer than one minute.
- Other overhead costs (rent, etc.) are not quantifiable.

As part of the development of this proposal, the department contracted Smartnet Pty Ltd, a business and technology advisory company, to:

- analyse the proposed changes
- map out the full range of SIM activation scenarios

[26] AMTA figures provide this figure as $5.70 per SIM, which has been adjusted for inflation.

[27] Calculations used data for 'Customer Contact Officer Level 2' wages, which are provided at $706.10 per week; Source: Fair Work Australia, *MA000023 - Contract Call Centres Award 2010*, http://www.fwc.gov.au/documents/modern_awards/award/ma000023/default.htm (as at 12 February 2012)

[28] Calculations used data for 'Customer Contact Officer Level 2' wages, which are provided at $706.10 per week; Source: Fair Work Australia, *MA000041 – Telecommunications Services Award 2010*, http://www.fwc.gov.au/documents/modern_awards/award/ma000041/default.htm (as at 13 February 2012)

[29] The actual DVS verification generally takes 1-5 seconds.

- develop a prototype online verification system that connects to the DVS and a service provider's activation system.

Smartnet's analysis shows that DVS costs will be minimised if service providers connect to the DVS through an intermediary service. If all or most service providers adopt such models, it could eliminate the cost of acquiring or developing multiple solutions, as well as the costs incurred to adequately test, host and support a range of individual solutions. Without the use of intermediary services, the greatest burden will likely fall on small and medium-sized service providers and potentially, government agencies managing services such as the DVS and VEVO, which may have to manage a large number of disparate users.

5.4.2. Benefits

This approach is expected to result in the following benefits:

- An estimated 30 000 third party retailers will no longer be required to undertake identity verification at the point of sale[30].
- Efficiencies for service providers resulting from the use of online identity verification and allowing identity verification through the use of existing practices (for example, courier delivery).
- More timely and efficient retrieval of information for law enforcement and security agencies, as information will be stored electronically rather than in hardcopy.
- Alignment of the identity verification process with the process to collect information for the Integrated Public Number Database, which also occurs when the SIM is activated.
- Improved privacy for consumers since third party retailers will no longer be required to sight or record identity information at the shopfront.
- A higher level of confidence regarding a person's identity as information provided will be verified using trusted sources such as the DVS.
- Control will rest with the mobile service provider that is accountable under the Telecommunications Act.

Table 5 below outlines the estimated cost per SIM and the savings that this option would bring to service providers.

[30] AMTA submission, Productivity Commission's *Annual Review on Regulatory Burdens,* February 2009, http://www.pc.gov.au/__data/assets/pdf_file/0019/86302/sub005.pdf

Table 5: Estimated recurring identity verification costs for service providers per SIM

Current requirements	$6.25
Proposed requirements	$2.15
Savings	**$4.10**

The above estimates are based on the assumptions and calculations outlined under **Table 4**.

The working group accepted that the proposed arrangements would not overcome all of the concerns of law enforcement and security agencies. However, it agreed that they will improve the current arrangements considerably and make it much more difficult for people to obtain and use a prepaid mobile phone with false identification.

Smartnet found that significant benefits to the digital economy and identity security would flow from maximising the use of the DVS for identity verification by businesses. It proposes that the reason for this is because it will eliminate current paper-based inefficiencies, help drive online productivity and improve the protection of personal information by reducing opportunities for uncontrolled copying and use.

5.5. Option 4b: Allow service providers to use identity verification methods at the point of activation, as well as the existing method

5.5.1. Costs

The cost components of this option are expected to be similar to Option 4a, however, the added flexibility provided to service providers under this option are expected to lower implementation costs. Providers will be able to implement the new methods according to their business requirements and their internal budget and IT upgrade cycles.

It is recognised, however, that some benefits may not be completely realised in the short-term, since the pace of adoption of the verification methods is likely to differ amongst service providers.

For example, consumer privacy is one area of concern that has been identified in the current arrangements. While the proposed arrangements are expected to improve the privacy of consumers, if service providers are slow to adopt parts of the proposed arrangements then the privacy concerns of the existing point of sale method will remain for longer.

Additionally, this inconsistent adoption rate will not only result in law enforcement and security agencies not having access to the improved retrieval methods under the proposed new methods, but will mean that these agencies will be required to engage different access methods for service provider data. This will likely have flow-on effects for their operation and may increase the associated administrative overheads.

The benefits of the new point of activation verification methods will also be delayed for those businesses who do not immediately adopt the new methods. Additionally, the high costs to industry of the existing method will be maintained.

Staged implementation will also mean that customers are likely to experience different identity verification processes depending on the provider they use.

5.5.2. Benefits

Implementation of private sector access to the DVS is currently in its early stages. A number of matters need to be finalised before the DVS can be used by industry, including the transaction price (which is subject to ongoing negotiations with states and territories), approval processes, and service and support arrangements. It will also take time for service providers to develop and test the necessary systems to connect to the DVS.

In order to avoid the risk of implementation of private sector access to the DVS delaying the new identity verification arrangements for prepaid mobiles, this option would allow service providers to adopt the new verification methods as they become available, or to maintain their current methods in the short-term. This modular design would afford service providers greater flexibility, allow them to adopt some verification methods sooner, and is expected to result in less transition issues.

Other benefits are expected to be the same as those under Option 4a. However, it is recognised that some benefits may not be completely realised in the short-term, as discussed above.

6. Consultation

The department and AGD co-chair the Commonwealth and Industry Telecommunications Experts Group. The group considered the issues relating to prepaid mobile service identity verification in June 2009, and unanimously agreed on the need to review the requirements to ensure that the policy objectives are met effectively and efficiently. The department agreed to lead a first-principles review in consultation with relevant stakeholders.

In September 2009, the department established a working group under the auspices of the Experts Group to address these concerns. The Prepaid Working Group comprised representatives from the department, AGD, the ACMA, AMTA, the Office of the Australian Information Commissioner, the Australian Federal Police, Telstra, Optus and Vodafone Hutchison Australia.

The working group considered various options, from removing identity verification requirements for prepaid mobile services completely, to a more stringent face-to-face identity verification process. It found that aligning the identity verification process with the activation of the service would appropriately place control with those who bear the compliance risk — i.e. telecommunications providers — and create a range of efficiencies.

In June 2011, the Experts Group endorsed a proposal by the working group which would see prepaid mobile customers able to verify their identity either online or over the phone when activating the service, while maintaining the option to verify their identity face-to-face. This approach is outlined under Option 4a above.

The department has subsequently consulted members of the working group, consumer groups (through the Australian Communications Consumer Action Network), and smaller mobile phone providers, including MVNOs.

The groups are generally supportive of the proposal subject to the implementation details. Industry has expressed concern that there should be cost effective access to verification services,

particularly the DVS. Consumer groups have emphasised the need to continue supporting groups who may have limited identification documents and to protect consumers' privacy.

In response to the concerns expressed by industry, the department has developed Option 4b, which adds additional elements of flexibility to Option 4a as developed by the Prepaid Working Group. Option 4b seeks to address the concerns that stakeholders raised with regards to adoption schedules and the potential costs involved with adoption of the entire regime by a designated cut-off date. This option allows industry to continue with the current arrangements in the short-term or adopt the new verification methods as they become available. The ACMA will consult on further implementation details during the development of its amendments to the Determination.

The proposal takes into account the needs of groups who may have limited identification documents and has been designed to improve the privacy of prepaid mobile customers.

The department also commissioned the preparation of an independent Privacy Impact Assessment and included provisions relating to privacy in its amendments to the *Telecommunications Regulations 2001*. The proposed arrangements offer considerable privacy improvements compared to the current arrangements.

7. Conclusion and preferred option

Option 1, maintaining the status quo, is not considered to be a viable option due to the numerous long-standing concerns raised by industry, law enforcement and security agencies and consumers.

Option 2, removing the requirement for service providers to verify the identity of their prepaid mobile service customers, is not viable as law enforcement and security agencies have stated that this would adversely affect their ability to investigate persons of interest and allow persons of interest to purchase mobile services anonymously.

In consideration of Option 3, improving the current face to face regime, the Working Group acknowledged that past efforts had not been effective, that the scope for improvement was very limited and it would not effectively address the needs of industry and law enforcement and security agencies.

Option 4a addresses the concerns outlined under 'Problems' above and provides a convenient method for prepaid mobile customers to verify their identity. It streamlines the verification process by only requiring customers to verify their identity at the point of activation. This is in contrast with the status quo, in which customers must verify their identity at the point of sale and provide the same information at the point of activation. Option 4a achieves this by providing service providers with the tools to verify identity using a range of methods such as verifying government-issued documents through the DVS, using a 'trusted' email address ending in ".gov.au" or ".edu.au", or verifying an account with a financial institution.

However, service providers have indicated that the mandatory transition proposed under this option may result in implementation challenges, given their differing budget cycles and operational capacities.

This option also relies on the schedule for the expansion of the DVS to the private sector, which is yet to be finalised. Option 4a is reliant on a completed DVS being available for private sector use, and until this is realised, this option cannot be implemented. AGD has indicated that there

may be a significant delay from the time a service provider applies for access to the DVS to the time it may begin verifying documents.

Option 4b seeks to provide service providers with the benefits of Option 4a while also providing them the flexibility to adopt new methods according to their business requirements. This will assist in implementation and will allow service providers to adopt new verification methods as they become available prior to the expansion of the DVS to the private sector.

However, it is possible that the voluntary adoption model of Option 4b may result in an inconsistent approach to identity verification in the short term, and may mean that some of the expected benefits may not be realised straight away.

On balance, the preferred option is Option 4b, given its implementation benefits. It is recognised, however, that maintaining the two systems in parallel in the short-term may have some disadvantages.

Given this, implementation under this option will be monitored with a view to removing the existing point of sale arrangements at a later date.

8. Implementation and review

As described above, it is proposed to offer the new identification verification requirements in parallel with the existing methods, as described in Option 4b. This would help to avoid the risk of implementation of private sector access to the DVS delaying the new identity verification arrangements for prepaid mobiles and to provide greater flexibility to service providers regarding the schedule of adoption of new identity verification methods.

This modular design would afford service providers greater flexibility, allow them to adopt some verification methods sooner, and is expected to result in fewer transition issues.

The *Telecommunications Regulations 2001* have been amended to allow the ACMA to amend its Determination. The ACMA will need to amend its Determination in order to enable service providers to implement the proposed arrangements.

It is proposed that adoption of the new verification methods will be assessed two years after the ACMA's Determination has been amended. At that time, the removal of the existing point of sale arrangements would be considered.

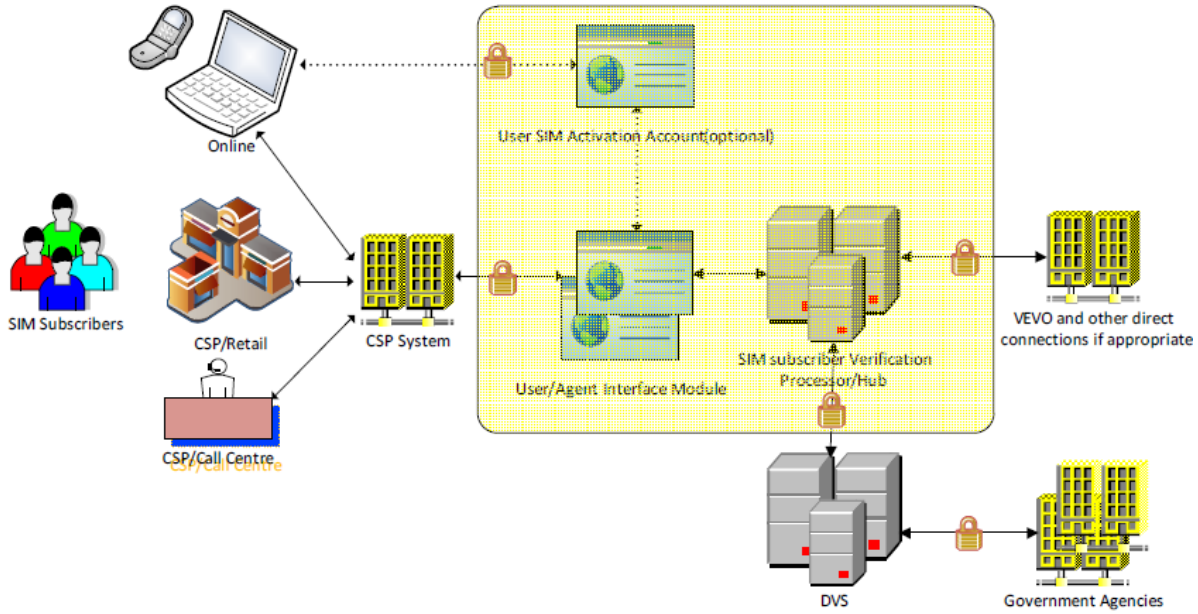
DVS usage levels and the costs associated with service provider access to the DVS will be analysed prior to any decision to remove the existing identity verification methods.

That being said, it is proposed that identity verification at a service provider's shopfront would be retained as per the working group proposal, even if the existing point of sale method is removed. This is to allow customers who are not able to utilise the new online methods to still purchase prepaid mobile services and fulfil the identity verification requirements.

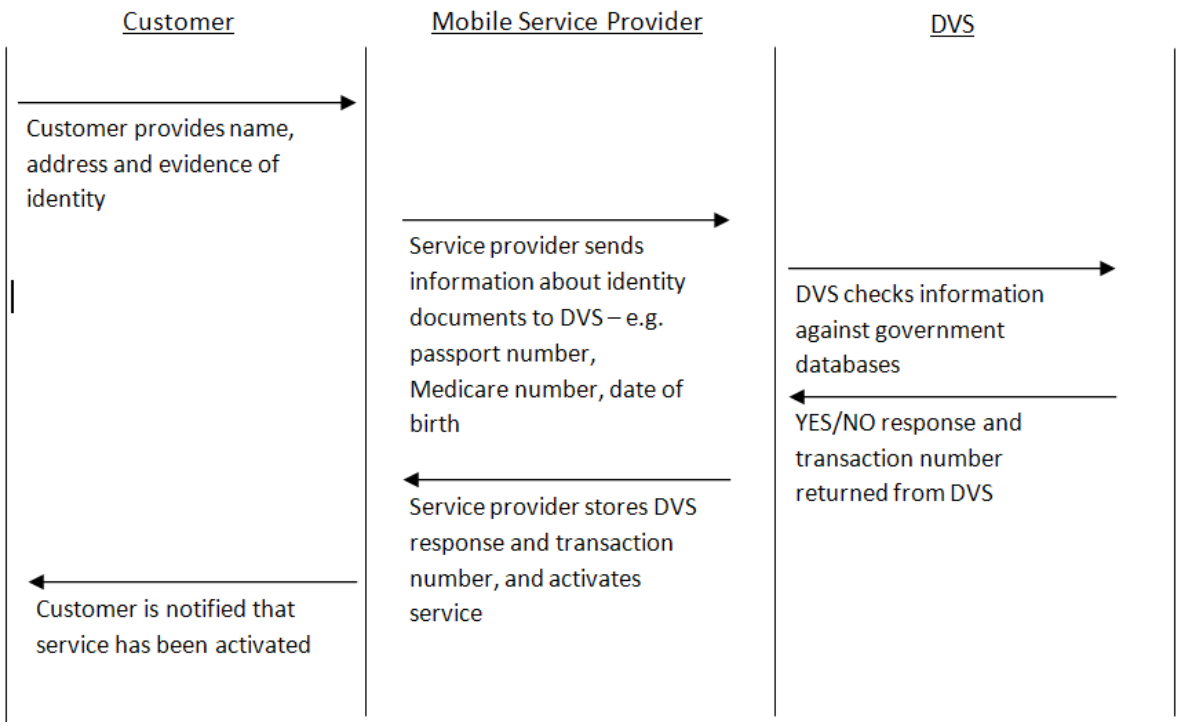
Implementation will be monitored by the ACMA, which will also be responsible for enforcement of the Determination.

A. Appendix

A.1. Diagram 1: Overview of the one-step prepaid SIM verification solution using the DVS and VEVO



A.2. Diagram 2: Information flow for identity verification using the DVS



A.3. Table 1: Expected cost components for service providers of the proposed arrangements compared to the existing arrangements

	Implementation costs	**Ongoing costs**
Current arrangements (point of sale)		
Point of sale form	• not available – first implemented in 2008.	• estimated by industry in 2009 to be $10 million per year to service providers – includes printing of forms, manual verification by retail assistants, postage and storage. • industry also estimated that the entire regime costs industry and their third party retailers $26-$27 million. • cost of verification per SIM estimated by industry in 2009 to be $5.70
Proposed arrangements (point of activation)		
Bank account verification	• some changes to processes and systems	• funds deposited into a bank account (a few cents) • other costs will depend on the degree of automation
Credit card/EFTPOS sale	• minor record-keeping changes – service providers will utilise their existing credit card and EFTPOS transaction process	• no additional cost expected
DVS	• application fee • connection fee • integration with the service provider's existing infrastructure • development and testing costs	• individual transaction fee (may vary according to volumes and whether providers connect to the DVS directly or through an intermediary service) • potentially an annual fee • internal hosting and support costs (subject to final pricing model)
VEVO	• no connection fee • system development and testing	• no individual transaction fee • no annual fee • hosting/support

Email verification	• changes to processes and systems	• negligible – process will be automatic
Courier delivery	• minor changes to processes and systems – service providers will utilise existing courier deliveries	• no additional cost expected
Existing post-paid account	• minimal changes to processes and systems	• negligible – the process could potentially be automatic
Face-to-face	• minor changes to processes and systems – essentially the current point of sale verification	• cost per verification expected to be the same as the current point of sale verification, however, total volumes are expected to be considerably less

A.4. Table 2: Draft fees and charges for DVS access

Scale A (Casual Rate model)

Annual Volume	Per calendar month	Per query charge
<400 000	<33 000	$1.75
>400 000 <600 000	>33 000 <50 000	$1.55
>600 000 <800 000	>50 000 <65 000	$1.35
>800 000 <1million	>65 000 <85 000	$1.15
>1 million	>85 000	$1.00

Scale B (Subscriber Rate model)

Annual Volume	Per calendar month	Per query charge
<400 000	<33 000	$1.65
>400 000 <600 000	>33 000 <50 000	$1.45
>600 000 <800 000	>50 000 <65 000	$1.25
>800 000 <1million	>65 000 <85 000	$1.05
>1 million	>85 000	$0.90