



Australian Government
**Australian Communications
and Media Authority**

Australia's regulator for broadcasting, the internet, radiocommunications and telecommunications

www.acma.gov.au

Improving Identity Check Processes for Pre-paid Mobile Services

© Commonwealth of Australia 2006

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Commonwealth. Requests and inquiries concerning reproduction and rights should be addressed to the Manager, Communications, Australian Communications and Media Authority, PO Box 13112 Law Courts, Melbourne Vic 8010.

Published by the Australian Communications and Media Authority

Canberra Central Office
Purple Building, Benjamin Offices
Chan Street, Belconnen
PO Box 78,
Belconnen ACT 2616

Tel: 02 6219 5555
Fax: 02 6219 5200

Melbourne Central Office
Level 44, Melbourne Central Tower
360 Elizabeth Street, Melbourne
PO Box 13112 Law Courts
Melbourne Vic 8010

Tel: 03 9963 6800
Fax: 03 9963 6899
TTY: 03 9963 6948

Sydney Central Office
Level 15, Tower 1 Darling Park
201 Sussex Street, Sydney
PO Box Q500
Queen Victoria Building NSW 1230

Tel: 02 9334 7700, 1800 226 667
Fax: 02 9334 7799

Contents

1	REQUEST FOR SUBMISSIONS	1
2	PRE-PAID MOBILE SERVICE OPERATING ENVIRONMENT	2
	2.1 Pre-paid mobile telephone services.....	2
	2.2 Credit checks and identity checks.....	2
	2.3 Consumer demand for pre-paid services.....	2
	2.4 Expanded distribution networks	3
3	PRE-PAID REGULATORY ENVIRONMENT	4
4	PROBLEMS ARISING FROM POINT-OF-SALE IDENTITY VERIFICATION PROCESSES	6
	4.1 Collection of information.....	6
	4.2 Reconciliation of collected and recorded identity information.....	6
	4.3 Industry costs	7
	4.4 Consumers	7
	4.5 Emergency services dispatch	7
	4.6 IPND accuracy	7
	4.7 Identity verification system.....	7
5	POSSIBLE REGULATORY RESPONSES	9
	5.1 Objectives of a revised identity checking process	9
	5.2 Available options	9
6	PROPOSED IDENTITY VERIFICATION PROCESS	10
	6.1 Summary of proposed changes	10
	6.2 Explanation of proposed changes	10
7	COSTS AND BENEFITS OF PROPOSED CHANGES	15
	7.1 Potential benefits.....	15
	7.2 Potential shortcomings.....	16
8	FUTURE OPTIONS FOR PRE-PAID IDENTIFY VERIFICATION PROCESSES	18
	8.1 Document verification service (DVS).....	18
	8.2 Telecommunications industry account verification system (AVS)	19
	8.3 Direct contact with evidence of identity issuing authority.....	19
	ATTACHMENT A: TELECOMMUNICATIONS REGULATION	20
	ATTACHMENT B: CASE STUDIES OF THE PROPOSED IDENTITY CHECKING PROCESS	23
	ATTACHMENT C: CASE STUDIES OF THE DVS, AVS AND MANUAL PROCESSES	25

1 Request for submissions

This paper outlines and seeks comment on a proposal to improve the identity checking processes that apply to pre-paid mobile services.

The reasons for the proposed changes, and an outline of revised identity checking process, are set out in this discussion paper. The proposal comprises a single, flexible identity verification process to replace the three alternative processes currently provided for. It removes identity checks from busy retail environments unrelated to the telecommunications industry and provides an expanded range of flexible identity verification options, which can be implemented outside those points of sale.

The pre-paid identity checking process is a complex area in which to satisfy the needs of all stakeholders. The need for robust identity checks of pre-paid mobile service users to serve community and national interest purposes might conflict with the need to foster a commercial environment in which consumers have ready access to telecommunications services and in which the telecommunications industry can function efficiently.

Accordingly, to further inform its consideration of the matter, The Australian Communications and Media Authority (ACMA) seeks submissions in response to the proposal set out in this discussion paper.

Subject to the views expressed in submissions, a new regulatory instrument will be made to introduce an improved identity checking process.

A primary consideration will be that changes to the legislated requirements and any corresponding changes to industry practices and systems be compatible with potential long-term solutions, such as those outlined in section 8 of this paper.

Submissions should reach ACMA by **Monday 3 April 2006**.

Please send submissions to cnit@acma.gov.au or fax (03) 9963 6983 or post to:

Manager
Community and National Interest
Australian Communications and Media Authority
PO Box 13112
Law Courts
Melbourne Vic 8010

2 Pre-paid mobile service operating environment

2.1 Pre-paid mobile telephone services

Pre-paid mobile phone services require users to pay in advance for the cost of their mobile phone calls. The cost of the calls is automatically deducted from the pre-paid credit balance that is stored in the user's pre-paid account. As credit reduces, the user has the option of purchasing another pre-paid service (which may involve obtaining a new telephone number and/or SIM¹ card) or, more commonly, re-charging the existing pre-paid service through the purchase of further credit.

The alternative to pre-payment is post-payment, which typically involves a contract with bills being sent to the customer at regular intervals in the same way as for most fixed line phone services.

The primary difference between pre-paid and post-paid services for the issue at hand relates to credit checking.

2.2 Credit checks and identity checks

When establishing a post-paid contract, carriage service providers (CSPs) conduct credit checks of the customer in order to ensure that he or she is able to fulfil the contractual obligation to pay the account for calls made in the billing period. While the purpose of these credit checks is to minimise business risk on the part of CSPs, it serves a dual purpose in that the process also verifies the identity of a customer.

As pre-payment eliminates the need for regular accounts or invoices to be mailed to the customer, there is minimal commercial need to collect and maintain accurate identity or address information for pre-paid customers.

2.3 Consumer demand for pre-paid services

In 2001-02, pre-paid services accounted for approximately 32.5 per cent of the mobiles market. At the close of the 2004-05 financial year, pre-paid services accounted for approximately 51 per cent of the 16.5 million mobile services currently in operation in Australia and represented the major area of growth in the mobiles market.

¹ Subscriber Identity Module: Each SIM within a GSM mobile phone is unique and corresponds to the subscriber's data. It enables mobile phone users to be identified by the mobile network as authorised customers entitled to make calls. GSM mobile phones will not work without a SIM, except to make emergency calls. CDMA (Code Division Multiple Access) mobile phones use different technology whereby the subscriber and handset data are integrated.

The stronger growth in pre-paid mobile services appears to be continuing, as consumers value having control over their mobile service expenditure and the ability to avoid lengthy contracts. The attractiveness of pre-paid services is also being enhanced as the value-added services that were previously only available to post-paid customers are being extended to pre-paid customers.

Given that pre-paid customers account for approximately 68 per cent of the mobiles market² in Europe, there would appear to be scope for further expansion of the pre-paid market in Australia. It is important that the policy objectives of the Determination are fulfilled in a way that does not unduly restrict the further development of the pre-paid market or consumers' access to pre-paid services.

2.4 Expanded distribution networks

To meet growing demand for pre-paid services, CSPs have significantly expanded their distribution channels by making pre-paid mobile products available from an increasingly wide variety of dealers and agents including convenience stores, petrol stations, video rental libraries, supermarkets, department stores and electronics retailers. Australian pre-paid SIM packs are also being marketed and sold on the internet for purchase prior to arrival in Australia.

Under their contractual arrangements with CSPs who supply pre-paid mobile services for sale, dealers and agents undertake identity verification processes on behalf of the CSPs. The rigour with which these checks are conducted is highly variable, and the environment in which they take place can be adverse to robust verification.

² 2004 European Mobile Outlook, quoted in Australian Communications Authority, Telecommunications Performance Report 2003-04

3 Pre-paid regulatory environment

Since 1997, purchasers of pre-paid mobile telephone services have been required to undergo an identifying process prior to activation of the service. It is principally for community and national interest purposes that accurate information about the users of pre-paid mobile services is required.

Accurate information about customers of pre-paid services supports law enforcement and national security agencies in their investigations and assists timely responses by emergency service organisations (i.e. police, fire and ambulance services) to emergency 000 calls from pre-paid services.

The *Telecommunications (Conditions for Allocation of Numbers) Determination 1997* (the Interim Determination) was made under the *Telecommunications Act 1991* to address law enforcement and national security concerns with the proposal of some carriage service providers (CSPs) to introduce (effectively) anonymous pre-paid mobile services.

The *Telecommunications (Service Provider – Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 1997* was made by the ACA under subsection 99(1) of the *Telecommunications Act 1997*, continuing the substantive effect of the earlier Determination.

Following a revision to the Determination in 2000, obligations on CSPs to collect and verify information about consumers of pre-paid mobile services are set out in the *Telecommunications (Service Provider—Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000*³ (the Determination).

The Determination is made under section 99 of the *Telecommunications Act 1997*.⁴ The provisions it contains, and any amendments made to it, must be confined in scope to the power conferred on ACMA by the *Telecommunications Regulations 2001* (the Regulations).⁵ The legislative basis for the identity verification requirement is outlined at Attachment A. The Regulations confers power on ACMA to make the Determination but do not compel it to do so.

The pre-paid Determination supports the obligation in Part 4 of Schedule 2 to the Act, which requires that CSPs contribute accurate information about customers to the integrated public number database (IPND), an industry wide database of all listed and unlisted public telephone numbers.

³ <http://www.comlaw.gov.au/ComLaw/Legislation/LegislativeInstrument1.nsf/0/D1488B5C1B1B7F6CCA256F8700816732?OpenDocument>

⁴ <http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401743?OpenDocument>

⁵ <http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401058?OpenDocument>

Since 1997, the Determination has provided for a point-of-sale process (now under Part 3) that requires CSPs to collect information about purchasers of pre-paid services at the time the service is purchased. CSPs are then required, for all purchases made other than by credit or debit card, to verify the person’s identity by viewing identifying documents such as passports or birth certificates.

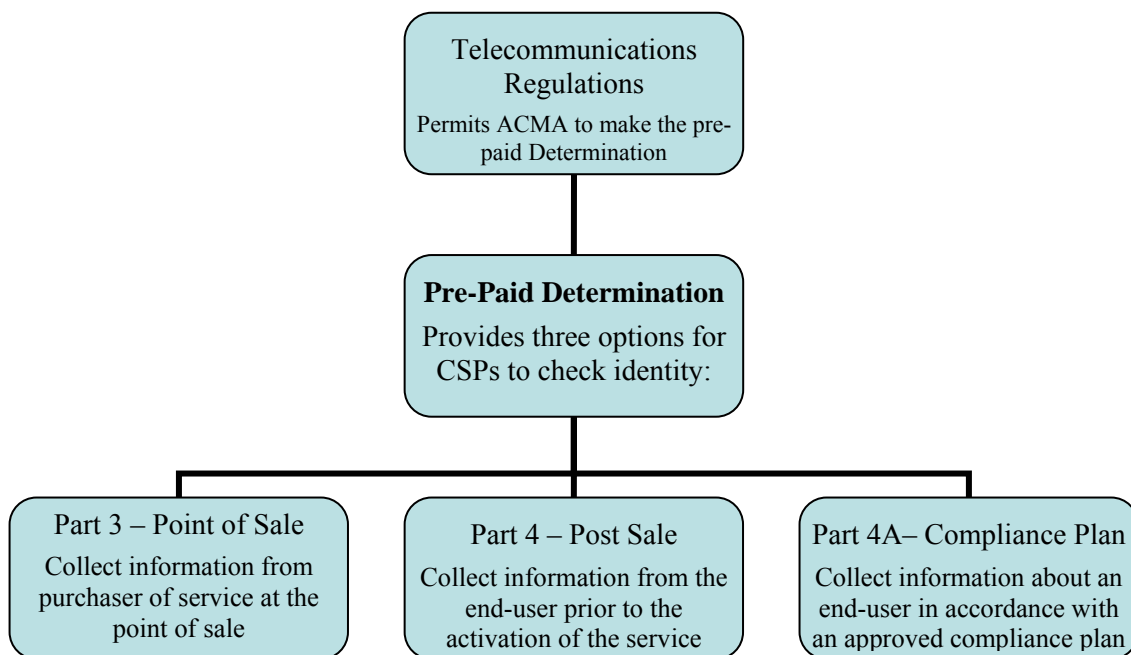


Figure 1 - Options for CSP compliance with the Determination

An amendment to the Determination in 2000 provided for an alternative post-sale identity verification process (under Part 4). Another amendment, in 2004, provided for another option, verification of identity in accordance with a process specified in an industry-developed compliance plan that has been approved by ACMA (under Part 4A).

However, while the Determination provides three alternative methods for verifying the identity of pre-paid users, industry has continued to operate exclusively under the original point-of-sale identity verification process.

4 Problems arising from point-of-sale identity verification processes

Stakeholders have identified a range of problems with identity verification of pre-paid mobile service users being performed at point-of-sale, as outlined below, which has prompted the development of the proposed changes outlined in section 6, below.

4.1 Collection of information

The business incentives for CSPs to collect identity and credit information about post-paid customers, such as the need to reduce the risk in extending credit, are notably absent in the pre-paid sector. The contractual requirement that is placed on agents and dealers to perform identity checks on behalf of mobile CSPs may be at odds with dealers and agents' core business activities, that is, sale of retail product.

The collection and documenting of identifying information by dealers and agents places obligations on a retail sector that may not:

- appreciate the importance of the identity verification requirements;
- have the experience or resources to perform the function adequately; or
- have the commercial incentive to fulfil the function to the standard required by the Determination.

4.2 Reconciliation of collected and recorded identity information

The information collected at point-of-sale is not always the information that is used to populate the CSPs' customer databases or the IPND. Completed identity verification forms are typically archived and CSPs use unverified data collected during a subsequent activation phone call or internet activation process to populate their own databases and the IPND.

The Determination, as it is currently constructed, does not prohibit this practice. This technical flaw in the Determination needs to be rectified because it leads to:

- collection of data about the purchaser of a pre-paid service who may not be the end user, since pre-paid services are often purchased as gifts or for dependents;
- inefficient business practices which may cost in the millions of dollars per annum for each major CSP;
- exploitation by mobile phone users who seek anonymity; and
- inaccurate data being included in the IPND.

4.3 Industry costs

The current point of sale processes appear inefficient and overly bureaucratic. Costs to CSPs include: contracting third-party dealers and agents to undertake checks; printing and distributing documentation to, and training of dealers and agents; monitoring and enforcing compliance with the contractual arrangements; receiving and archiving printed identity verification documentation; and collecting data separately at the point-of-activation. It would seem to be inherently more efficient to conduct identity checks only once, at the point of activation of a service.

4.4 Consumers

The point-of-sale identity verification process, as it is currently practised, typically requires consumers to submit personal details twice, once at point-of-sale and again at point-of-activation. Further, customers may be asked to provide personal details and evidence of identity (EOI) documents in a retail environment in which they may not have confidence that their privacy and identifying information will be appropriately safeguarded.

Consumer access to emergency services may be compromised if the information recorded about them in the IPND is inaccurate (see next item).

4.5 Emergency services dispatch

Emergency service organisations handling an emergency call have access to IPND information about the account holder of the service that is being used to make the emergency call. The IPND information includes the person's name and address, which can be used to rapidly dispatch an emergency service vehicle when the caller is at their address, or, if necessary, to verify a caller's identity.

Inaccurate IPND information can lead to delays in the dispatch of emergency services while correct information is verbally relayed to the emergency service operator. Verbal checking of address details can be compromised by the stresses inherent in reporting time-critical or life-threatening emergencies.

4.6 IPND accuracy

Reports from law enforcement agencies suggest that the quality of identifying information in the IPND relating to pre-paid services is significantly poorer than that for post-paid mobile or fixed telephone services⁶. While many of IPND errors are minor, the data inaccuracy is of significant concern because of its adverse impact on approved data users, such as law enforcement agencies, which use the data in their investigations of serious crime and terrorist threats.

4.7 Identity verification system

The lack of an accessible data source for identity verification away from the point of sale has hindered the use of the Part 4, post-sale process. As discussed in section 8, the Australian Government is developing means to verify identity online, but it is not clear that this will be

⁶ Some of the concerns raised regarding the accuracy of information about pre-paid customers appear to be justified, given that ACMA's 2005 audit of the IPND found that only 35.2 percent of mobile service records were categorised as 'highly accurate' compared to 79.3 per cent of fixed service records.

'Highly accurate' means that most address fields for the record are used and were a perfect match to the comparison address database. The audit also indicated that 96.8 percent of fixed service and 85.2 percent of mobile service records were highly useable, if not perfect.

deployed in the near term, or that the system will be extended to use by the communications sector.

5 Possible regulatory responses

5.1 Objectives of a revised identity checking process

The proposed changes to the Determination aim to establish a more effective and efficient set of processes for verifying the identity of pre-paid mobile customers. The policy objective that is served by the Determination, which remains unchanged, is for information about the identity of consumers of pre-paid mobile services to be collected and verified before the activation of those services.

Outcomes sought from the review of identity checking processes include:

- Improved compliance by industry with identity checking obligations;
- A reduction in industry compliance costs;
- An overall improvement in outcomes for consumers;
- Improved privacy protections for consumers:
 - i) improved accuracy of customer information in the IPND (in line with National Privacy Principle 7);
 - ii) secure data collection procedures to reduce the chance of mishandling customer information (in line with National Privacy Principle 4);
- Accommodation of foreseeable technological and other developments;
- No undue regulatory barriers on the sale of pre-paid services.

Submissions made in response to this paper, which recommend particular courses of action, should address these criteria.

5.2 Available options

ACMA has considered the problems outlined in section four in light of the review objectives above. In doing so, it has considered what regulatory response might be appropriate, including:

- the removal of the Determination altogether;
- immediate amendment; or
- postponing amendments until a national identification system is more fully developed.

ACMA is of the view that the Determination should be retained but that some immediate changes should be made to improve its operation. Those changes should be made in anticipation of broader initiatives to improve Australia's identity security framework.

6 Proposed identity verification process

6.1 Summary of proposed changes

An outline of the proposed changes to the identity checking process is provided below. The proposal represents a shift away from identity checking by third party dealers and agents at the point of sale, to verification by the CSP itself. It provides a single, flexible process, with an expanded range of verification options and an emphasis on remote identity checking.

There will be instances where identity verification will be difficult or inconvenient under this model. A number of alternative identity checking methods have been identified and additional proposals will be considered.

While the proposed changes are expected to be more efficient and effective, there may be some shortcomings and cost burdens on industry. Comments are invited on strategies addressing those issues, and ACMA will work with interested parties to address their concerns.

6.2 Explanation of proposed changes

The operation of the proposed process is shown in Figure 2. See Attachment B for case studies that are intended to illustrate the proposed process might work in practice.

Step 1: Customer obtains a pre-paid service

Consumers obtain a pre-paid service (such as a mobile phone SIM-card) from any number of outlets, such as CSP branded stores, supermarkets, petrol stations, or potentially even vending machines.

The pre-paid service would be in an inactive state, providing access only to the relevant CSP and the emergency call service.

Step 2: Customer contacts CSP to activate pre-paid service

To activate a pre-paid service, a customer would contact the relevant CSP and undergo an identity checking process.

If the customer obtained the pre-paid service at a branded CSP store or other outlet such as dealer or agent with direct access to the CSP's computer systems and databases, then the identity checks could be conducted in person at the time of purchase, as in this case it would likely also be the point of activation of the service. Alternatively, the customer could contact

the CSP by internet or phone, including using the mobile phone for which the pre-paid service was purchased.

Irrespective of the means of contact, the CSP would be required to collect identifying information about the customer as follows (and in line with current requirements).

- If the customer is obtaining the service for personal use, the CSP would collect the name and address of the customer.
- If the customer is obtaining the service for business purposes, then the CSP would collect the customer's name, the name and address of the business, and an identifying number for the business, such as an ABN or ACN.

Step 3: CSP records and validates customer information

As the customer provides the CSP the required information in person, by phone or internet, the information would be entered into the CSP's computer system.

CSPs are increasingly using software that checks the validity of names and addresses.⁷ It is proposed that address information would be validated at the time of entry into the CSP's database. Validation techniques are valuable for quality-checking data supplied by pre-paid users by helping to keep spelling mistakes and other inadvertent errors out of the IPND.

Step 4: CSP verifies identity

When the CSP has collected customer information and validated the address, it would be required to verify that the customer is the person she or he claims to be through one of five techniques.

Exemption for credit or debit card

There is currently an identity check exemption for pre-paid customers who pay for the service using a credit or debit card. This is because the identity verification processes undertaken by the financial sector when a person obtains a credit or debit card are more stringent and are therefore taken to have also met the identity verification obligations for pre-paid mobile phone services. It is proposed that this exemption would remain.⁸

Where a pre-paid service is paid for by a means other than by credit or debit card, identity verification against a reliable source would be required.

a Existing CSP accounts

Currently, the Determination allows for identity to be checked against a statement of account for fixed line telecommunications services.

A matter under consideration is an expansion of the range of telecommunications account information which can be used to verify identity to include, for example, post-paid mobile, internet and pay TV accounts.

⁷ It is important to distinguish validation from verification. Identity verification techniques attempt to ensure that the information collected about a person is true and correct. For example, to verify that John Smith is who he says he is it would be necessary to establish that John Smith actually lives at 360 Elizabeth Street in Melbourne and was actually born on 1 January 1980.

Identity validation, by contrast, checks that information provided *could be* true and correct. For example, validation of a user's address will determine that the address exists, not that the user actually lives there. For example, if a new subscriber submitted the following details – John Smith, 360 Elizabeth Street, Melbourne, Victoria, 3001 – validation software could check that: the name John Smith is a genuine name (eg. not 'Mickey Mouse'); the postcode for Melbourne is 3001; Melbourne is in Victoria; there is an Elizabeth Street in Melbourne; and there is a number 360 on Elizabeth Street.

⁸ It is beyond the scope of ACMA's Determination to address the broader issue of identity fraud where a person presents genuine identity documentation belonging to another person.

Financial accounts

In addition to verification through the credit or debit card exception, currently a pre-paid customer's identity may be verified against valid financial accounts, including in circumstances where the customer may have purchased the pre-paid service using cash or cheque.

ACMA is considering expanding the range of financial documents available to CSPs for identity verification to include B-Pay arrangements;

Evidence of identity (EOI) documents

Currently the CSP may inspect the EOI documents provided by a customer in order to verify the person's identity.⁹

It is proposed to revise the list of acceptable EOI documents, to the following:

Category A (single document required)

<ul style="list-style-type: none"> ▪ Australian passport ▪ Birth certificate ▪ Record of immigration status (eg. foreign passport and Australian visa) 	<ul style="list-style-type: none"> ▪ Australian driver licence ▪ Citizenship certificate ▪ Proof of Age card
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------

Category B (two documents required)

<ul style="list-style-type: none"> ▪ Medicare card ▪ Department of Veterans' Affairs card ▪ Births, Deaths and Marriages-issued marriage certificate ▪ Utilities or rates notice 	<ul style="list-style-type: none"> ▪ Change of name certificate ▪ Security guard licence ▪ Tertiary ID card ▪ Firearms licence
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------

It is proposed that the option of inspecting EOI documents would remain available in branded CSPs stores or dealerships that have the information technology systems in place to activate the service.

However, it is also proposed that this option would no longer be allowed in distributed sales outlets - such as supermarkets and petrol stations - that are not connected to CSPs' service activation systems.

b Previously verified identity

Currently the Determination does not require identity verification to take place prior to recharge or reactivation of the same pre-paid service where an identity check has already been performed.

It is proposed to expand this exemption to allow for the activation of new pre-paid services (for example, a pre-paid mobile service with a new number) by the same customer where an

⁹ Part 3 of the Determination currently requires CSPs to verify customer information using either one category A document (such as a passport or drivers' licence) or two category B documents (such as debit cards and Medicare cards) as listed in Schedule 2 to the Determination (see <http://scaleplus.law.gov.au/html/instruments/0/30/0/2004083001.htm>). Part 4 of the Determination requires CSPs to collect 30 points of identifying information (or 40 points where the customer has five or more active pre-paid services) about the end-user of a pre-paid service and match it to a reliable data source. As an example, the date of birth of the customer is worth 5 points. By contrast, the finance industry is regulated under the *Financial Transaction Reports Act 1988* (the FTR Act), which is required to perform 'the 100 points check' as prescribed in the *Financial Transaction Reports Regulations 1990* (the FTR Regulations).

identity check had been undertaken for the previous service and the details remain in the CSPs records. This option would require additional processes to ensure that the person purchasing the new service is the existing account holder.

Step 5: Alternative identity verification

A CSP may be unable to verify the identity of a customer using any of the methods in step 4, for example because a customer is too young to have a financial account; does not have access to their own EOI documents; finds it inconvenient or difficult to attend a store in person; or for some other reason.

To accommodate these types of situations, it is proposed that the identity of a second person may be checked in lieu of the user of the pre-paid service in a referee capacity. For example, a parent's identity could be verified for a service issued to a minor or the identity of a person associated with the pre-paid mobile user could be verified in lieu of the user. The financial sector's protocols with respect to referees and guarantors for consumer access to financial services may provide a useful model here.

Step 6: Activation of pre-paid service

Following the completion of adequate identity verification procedures, and provided that the CSP is satisfied that the customer has been accurately identified, the CSP may activate the pre-paid service to enable the customer to initiate and receive communications.

Currently, a CSP must not activate the service, or must deactivate a service, if it has reason to suspect that the identity information it holds is incorrect. These obligations will remain unchanged.

Step 7: Service not activated

Where a CSP is unable to verify the identity of a customer, the service cannot be activated.

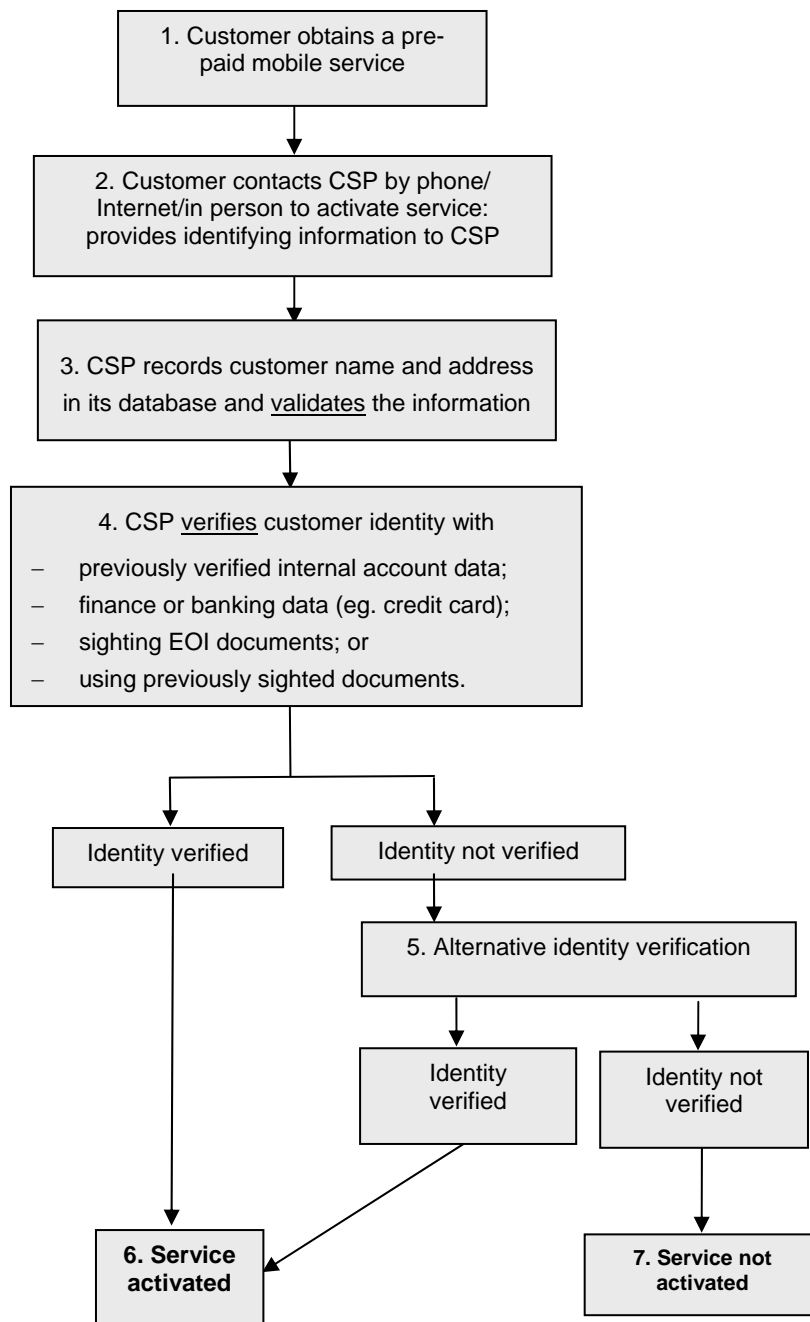


Figure 2 - Proposed identity verification process

7 Costs and benefits of proposed changes

7.1 Potential benefits

It is anticipated that implementation of the proposed changes to the identity checking process would result in a range of benefits for all stakeholder groups.

Some potential benefits are outlined below. Submissions are invited on whether the anticipated benefits are realistic and achievable.

7.1.1 *Carriage service providers*

- Lower cost of pre-paid service sales and distribution by eliminating need for printing and distributing paper documentation; staff training; and contractual provisioning and enforcement.
- Increased efficiency by eliminating duplication of data collection at point-of-sale and point-of-activation.
- More flexible sales and marketing opportunities for pre-paid services due to elimination of identity verification at point-of-sale.
- Reduced risk of regulatory breach due to greater control of a single, centralised, identity verification process that is no longer reliant on distributed network agents.

7.1.2 *Consumers*

- Improved personal privacy, with identification documents produced only once and only to the staff of the CSP (rather than to sales staff in distributed sales networks).
- A faster, more efficient activation process in the majority of cases.
- More effective emergency service dispatch due to better quality data being provided to the IPND by the pre-paid mobile CSP and, in turn, provided to the emergency service organisation in conjunction with an emergency call.

7.1.3 *Data users*

- Improved accuracy of identity data and validated address data recorded in the IPND and, as a consequence, improved quality of information available to emergency service organisations; law enforcement agencies; and directory producers.

7.1.4 *Distributed sales networks*

- Removing the obligation on dealers and sales staff at the distributed sales networks (petrol stations, supermarkets, etc.) to perform identity checks at the point-of-sale, thereby improving the efficiency of the retail process by:

- reducing the time required to complete sales;
- eliminating the need to train staff to complete identity checks; and
- removing the time and cost impost of forwarding completed identity check documents to the relevant CSP.

7.1.5 Regulatory authority

- Consolidating identity verification processes with CSPs would enhance ACMA's capability to regulate effectively in this area.¹⁰

7.2 Potential shortcomings

Implementation of the proposed verification system will come at some initial (and possibly ongoing) cost to industry and may not uniformly benefit all consumers.

Some potential impacts and costs are outlined below. Comment are invited on these impacts and any other potential adverse impacts and suggested remedies. In particular, CSPs are invited to provide detailed information on the anticipated costs of the proposed identity verification process, in comparison with current costs.

7.2.1 Carriage service providers

- There will be costs associated with modifying business systems to accommodate revised identity verification processes, although this should be offset by reduced compliance costs over time.
- CSPs with a large post-paid customer base are likely to receive greater benefit than other CSPs from some proposed process such as identity verification against existing service accounts.

7.2.2 Consumers

- Primary reliance on electronic identity verification may be perceived as establishing a two-tier system which disadvantages minors and others with limited access to acceptable EOI documents and/or electronically recorded identity documents. These potential barriers would be consistent with those in other sectors that require identity verification to access services, such as financial transaction services.
- Where existing credit or account data is unavailable, a requirement for customers to attend a CSP store in person could be inconvenient or even very difficult for those in rural areas or those with mobility impairment.

7.2.3 Data users

- Although unlikely, there is potential for automated systems to be programmed to provide the IPND with default data if the data entry, address validation or identify verification processes are not properly completed. The risks for data users (such as law enforcement agencies and emergency service organisations) associated with mass default entries into the IPND of inaccurate identifying information should be offset by ready detection of systems-based errors and more direct regulatory action by ACMA in response to any CSPs who breach the revised Determination in this (or any other) manner.

¹⁰ The sanctions available to ACMA under the Act where a service provider is found to be non-compliant include:

- issuing a formal warning (section 103);
- issuing a remedial direction (section 102);
- seek a court order in relation to an enforceable undertaking (section 572C); and
- taking action in the Federal Court to recover a pecuniary penalty of up to \$10 million for each instance of non-compliance (section 101).

7.2.4 Distributed sales networks

- The purchase of pre-paid services from distributed sales outlets may decline with respect to customers who know that they will be unable to complete the activation process over the phone or by internet and may be required to enter a CSP branded shop to present identifying information. Any such loss of custom should be offset by savings achieved through relief from contractual obligations to undertake identity checking in a retail setting.

8 Future options for pre-paid identify verification processes

While this paper identifies a number of improvements that can be made to the identity checking for pre-paid services in the short-term, it is intended the outlined processes would be compatible with possible longer-term solutions involving access to online, real time identity verification systems.

See Attachment C for case studies that illustrate the following processes in practice.

8.1 Document verification service (DVS)

In accordance with its National Identity Security Strategy, the Australian Government is developing a document verification service (DVS) for inter-government agency use. A prototype DVS was launched on 7 February 2006.¹¹

The DVS will provide an online interface between an agency seeking to verify a person's identity and the agency that issued the consumer's EOI document including State registries of births, deaths and marriages, State departments of road transport and the Australian passports office.

An approved DVS user would provide a consumer's name and EOI document identifier (such as a driver licence number) into the online interface and receive a positive or negative response from the database of the relevant issuer of the EOI document. For example, the entry of a driver's licence number into the DVS would automatically seek confirmation from the relevant road transport department's database. The DVS would provide the CSP with either 'YES' or 'NO' response depending on whether the identifying data was correct.

The DVS has the potential to transform the ability of the telecommunications industry to perform its statutory obligations to check the identity of pre-paid mobile phone users. However, future extension of the DVS to the private sector is by no means certain and, even if access is afforded, it may not occur for several years.

Although neither the customer nor the mobile CSP would at any point in the transaction have access to the content of EOI databases that underpin the DVS, perceived consumer privacy implications may influence the availability and/or timing of the DVS to the telecommunications industry for the purpose of checking the identity of pre-paid mobile service users.

¹¹ http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases_2006_First_Quarter_7February_2006_-_Document_Verification_prototype_central_to_identity_protection_-_0102006

8.2 Telecommunications industry account verification system (AVS)

Due to the diversity of telecommunications industry, an account verification system (AVS) service could be developed that draws on collective records of the telecommunications industry. Rather than each CSPs being confined to drawing on its own customer database, it would be able to draw on the records of other industry participants to verify pre-paid service users' identities.

A telecommunications AVS could be set up in a similar fashion to the proposed Australian Government DVS, namely, an online data challenge-response system.

The degree to which an AVS can be integrated with CSPs' existing business systems (and potentially the DVS) may dictate the overall costs and benefits to industry. However, industry could control the costs of developing and accessing an AVS, while it would have little influence over the cost of access to a DVS (should that become available to the telecommunications sector for this purpose).

Commercial sensitivities surrounding any form of access to competitors' customer data would require careful and ongoing management. Consumer privacy issues would also need to be directly addressed.

Industry representative groups such as the Australian Communications Industry Forum (ACIF) or the Australian Mobile Telecommunications Association (AMTA) could be instrumental in sponsoring discussions to scope an industry-specific AVS. Potentially, industry could leverage additional benefit by incorporating established systems, such as the ACIF-developed Electronic Information Exchange.

8.3 Direct contact with evidence of identity issuing authority

In situations where a customer is unable to attend a CSP store in person, it may be possible for a CSP to verify the customer's identity with the EOI document-issuer by phone. This type of arrangement was trialled in 2000 between Westpac and the New South Wales registry of Births, Deaths and Marriages.¹²

In this scenario, a CSP would telephone an EOI document issuer to request that the pre-paid customer's identifying details be checked against the EOI issuer's records. This procedure would necessarily entail the resolution of privacy issues, including the CSP obtaining the formal permission of the pre-paid mobile service user to seek disclosure from the EOI issuer.

CSP would need to develop relationships with EOI issuing authorities and introduce systems and protocols to support the identity verification process. Potentially, CSPs could collectively negotiate identity verification procedures with EOI issuers, possibly through AMTA or another representative body.

This option may work as an interim measure in advance of potential telecommunications access to the DVS and as a fallback measure should the DVS subsequently be made available to the telecommunications sector.

¹² Testimony from Mr Chapman of the Australian Banker's Association to the House of Representatives Standing Committee on Economics, Finance and Public Administration: *Tax File Number Inquiry: Discussion*, 10 Feb 2000, at p 101, <http://www.aph.gov.au/hansard/rep/commtee/R665.pdf>.

Attachment A: Telecommunications regulation

Telecommunications Act

The *Telecommunications Act 1997*¹³ (the Act) is the primary legislative instrument for the telecommunications industry. It imposes a range of obligations on carriers and CSPs, including internet service providers, and requires ACMA to monitor compliance with those obligations.

The overarching objectives of the telecommunications regulatory policy framework (section 3 of the Act) include the promotion of:

- the long-term interests of end-users of carriage services;
- the efficiency and international competitiveness of the telecommunications industry;
- the supply of diverse and innovative carriage and content services;
- the effective participation of all sectors of the industry in markets; and
- appropriate community safeguards in relation to telecommunications activities.

Various provisions in the Act, and in its subordinate legislation, place obligations on CSPs with respect to collecting, providing and disclosing information about their customers to authorised agencies for approved purposes.

Part 4 of Schedule 2 to the Act requires that CSPs contribute to the maintenance of the IPND, an industry wide database of all listed and unlisted public telephone numbers. Entries also include information associated with each number such as the customer's name and address and the name of the CSP. This data may only be accessed and used for approved purposes such as providing directory services, producing public number directories, and assisting law enforcement agencies or emergency service organisations.

The *Telecommunications (Emergency Call Service) Determination 2002*¹⁴ was made by ACMA's predecessor, the Australian Communications Authority (the ACA), under the *Telecommunications (Consumer Protection and Service Standards) Act 1999*.¹⁵ It supports the operation of the emergency call service by requiring CSPs to provide the IPND Manager with correct information about their customers. When a call is made to the emergency call service, the name and address information associated with the number from which the call is being supplied from the IPND to the relevant emergency service organisation (police, fire or ambulance service) to facilitate the rapid dispatch of an emergency vehicle.

Part 14 of the Act requires carriers and CSPs to provide assistance to law enforcement and national security agencies. A vital part of each CSP's preparations to assist law enforcement agencies is the obligation to maintain accurate records of their customers' personal details. Carriers and CSPs are called upon to provide a range of customer information to law enforcement agencies for purposes specified under the Act such as the enforcement of the criminal law, the protection of public revenue, or in relation to threats to a person's life or health. Customer information recorded by the CSP or submitted to the IPND is delivered upon lawful request to authorised agencies.

¹³ <http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401743?OpenDocument>

¹⁴ <http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200506943?OpenDocument>

¹⁵ <http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401807?OpenDocument>

Telecommunications Regulations

Subsection 99(1) of the Act provides that ACMA may make a written Determination setting out rules that apply to service providers in relation to the supply of specified carriage services and/or specified content services.

Subsection 99(3) of the Act requires that such Determinations must relate to a matter specified in the *Telecommunications Regulations 2001*¹⁶ (the Regulations).

The Determination providing for pre-paid mobile service identity checks is made under Division 3.2 of the Regulations.

Identity Checks for Pre-paid Public Mobile Services Determination

The current *Telecommunications (Service Provider—Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 2000*¹⁷ is preceded by several other Determinations which shared the same objective.

The *Telecommunications (Conditions for Allocation of Numbers) Determination 1997* (the Interim Determination) made under subsection 242B(3) of the *Telecommunications Act 1997*¹⁸ to address law enforcement and national security issues associated with the proposal of some CSPs to introduce effectively anonymous pre-paid mobile services.

The *Telecommunications (Service Provider – Identity Checks for Pre-paid Public Mobile Telecommunications Services) Determination 1997*¹⁹ was made by the ACA under subsection 99(1) of the 1997 Telecommunications Act, continuing the substantive effect of the Interim Determination. The 1997 Determination was made pursuant to the *Telecommunications (Service Provider Determinations) Regulations 1997*.

The 1997 Determination provided for a point-of-sale process that required CSPs to collect information about purchasers of pre-paid services, including name and address, at the time the pre-paid service is purchased and to verify that information by viewing identifying documents such as passports or birth certificates.

In 2000, the 1997 Determination was repealed and a new Determination was made by the ACA.

The 2000 Determination retained the point-of-sale process and added a new, alternative process at Part 4. The Part 4 process provided for CSPs to obtain identifying information about the end-user from a database held by the CSP or another person, or from documents seen by the CSP. The 1997 Determination was made pursuant to the *Telecommunications (Service Provider Determinations) Regulations 1997*.

Efforts by industry to gain access to a single data source to verify identity information were not productive. As a result, CSPs have not utilised the Part 4 point-of-activation process.

In May 2004, the ACA amended the Determination to enable each CSP to develop its own, tailored, identity verification processes for pre-paid mobile services and to set this process out in a Compliance Plan. If ACMA approved such a Compliance Plan (after consultation with agencies), a CSP could utilise the identity processes set out in the Plan instead of the

¹⁶ <http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200401058?OpenDocument>

¹⁷ <http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200506949?OpenDocument>

¹⁸ <http://www.comlaw.gov.au/ComLaw/Legislation/Act1.nsf/asmade/bytitle/77066565F1AD05BACA256F7200179E16?OpenDocument>

¹⁹ <http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200506949?OpenDocument>

Part 3 or Part 4 processes. The 2004 amendment to the pre-paid Determination was made pursuant to Division 3.2 of the Telecommunications Regulations 2001.

While the ACA has considered draft Compliance Plans submitted by industry, to date it has not approved any Plans because of the need to ensure that existing standards of identity verification are maintained or improved, not weakened.

Attachment B: Case studies of the proposed identity checking process

CASE STUDY: EVIDENCE OF IDENTITY PRESENTED IN CSP SHOP

Brothers Milo and Ellis arrived in Australia for a working holiday. They each purchase a pre-paid mobile service (in the form of a SIM-card) at the airport newsagency and insert the cards into their mobile phones. Milo paid using his credit card and Ellis paid by cash.

Milo phoned his Australian CSP to activate the full mobile service, providing the operator with his name and contact address in Australia. The operator determined from the CSP's own records that Milo had paid for his pre-paid service using a credit card and activated his account immediately.

Ellis also phoned his Australian CSP to activate the full mobile service. Because he had not paid by credit (or debit) card, Ellis had to provide his name and contact address in Australia. Because he did not have a credit card or Australian bank account and did not have a telecommunications account in Australia, the CSP is unable to verify his identity.

Ellis is required to go into a branded shopfront of the CSP to present photo identification. There is no branded shopfront at the airport and it is out of standard shopping hours, so Ellis has to wait until he is in the city the following day to activate his service.

The following day Ellis goes into one of his CSP's shops and presents his passport. The assistant sights Ellis' photo ID and records his passport number into the CSP's database. The CSP activates Ellis' service.

Milo and Ellis' names and Australian contact address details are provided by their CSPs to the IPND Manager for inclusion in the IPND.

CASE STUDY: FINANCIAL ACCOUNT VERIFICATION

Sadie purchases a pre-paid service from her local supermarket, paying for the service with her groceries. She leaves the supermarket without providing any kind of identifying information.

At home, Sadie logs on to the web address provided on the packaging of her pre-paid service. She enters the identification number for the service as well as her name, address and other personal information as required by the CSP. Sadie accidentally misspells her street address but the CSP's address validation software picks up her mistake and prompts her to correct it.

The website then prompts Sadie to provide information contained in one category A document or two Category B documents. Sadie provides her credit card number (and also grants authority to the CSP to debit her card each month to top up the credit for her service).

The CSP's computer system receives the credit card details and checks that the credit card is valid. As the card is valid, the system registers that Sadie's identity has been verified and allows credit to be allocated to her service.

Sadie's name and address information is provided by her CSP to the IPND Manager for inclusion in the IPND.

The same process would apply if Sadie activated her service by phoning the CSP and spoke to a (manual or automated) telephone activation service.

CASE STUDY: REFEREE IDENTITY VERIFICATION

Ewen has received a pre-paid mobile phone for his thirteenth birthday from his family. The phone came with a pre-paid service card but the service has not been activated.

Ewen logs onto the CSP's internet site to activate the pre-paid service. He enters his name and address as requested but is unable to complete the online identity verification form because he does not have relevant accounts in his own name or any other acceptable form of identity.

Having exhausted other options, the CSP's online activation service prompts Ewen to seek a referee to provide identifying information for verification. Ewen's mother, Elaine, provides her name and her landline number.

The CSP's computer system checks the records it holds about Elaine, confirming that it has record of her name and address and that her landline accounts are regularly paid. The CSP records Elaine's details as referee for Ewen and activates Ewen's service.

Ewen's name and address details are provided by the CSP to the IPND Manager for inclusion in the IPND.

Attachment C: Case studies of the DVS, AVS and manual processes

CASE STUDY: DOCUMENT VERIFICATION SYSTEM (DVS)

Jack had lost his mobile phone at university so was pleased to find that his Christmas stocking contained a new mobile phone, complete with inactive pre-paid mobile service (SIM-card). Jack notes on the instructions about how to activate the phone and the types of identifying documents that would be accepted for the identity check that preceded activation. He chooses to use two Category B documents, his Medicare card and a Tertiary ID card.

Inserting the pre-paid service card into his phone, Jack phones his new CSP. The CSP's automated activation service asks Jack to state his name and address. It then reads a privacy statement and asks Jack to provide verbal permission to use his personal identifying data to undertake an identity check with the selected EOI issuing authority. Jack provides his permission which is recorded by the CSP.

The telephone activation service then instructs Jack to identify the type of ID that he will be presenting and to provide the ID reference number. Jack enters his Medicare card number. The CSP's system logs Jack's name and Medicare number and interfaces with the DVS, which in turn interrogates the Medicare database. Jack's name and Medicare number correlate, so the Medibank database sends a 'YES' response to the DVS. The positive response is logged in turn by the CSP's automated system.

The CSP's system then asks Jack to state the number of a second identifying document. The same process then applies, with the DVS interrogating the university student database. This time the system comes back with a 'NO' response. Jack is puzzled because he has had the same student number for two years and never had a problem like this before.

The CSP's system asks Jack whether he wants to enter the details of another identifying document or to speak to a CSP customer assistant. He chooses to speak to the assistant and advises her that his student ID number is correct. The CSP checks to see that the number was correctly keyed into the CSP system that interfaces with the DVS. The number had been entered correctly, so the CSP informs Jack that it is the university's own database which is not recognising the number in relation to his name but, since the CSP does not have access to the university's database, Jack would need to contact the university himself to sort out the problem with his student identity number.

She asks Jack whether he has another form of ID that could be used to activate the pre-paid mobile service.

Jack says he would look for his birth certificate but that it might take a while. The CSP gives Jack a priority phone number to ring back on so that he can continue with the second part of the activation process from where it had been suspended.

When he finds his birth certificate, Jack rings his CSP back and provides details and birth certificate number. The DVS checks Jack's details against the relevant State's Births, Deaths and Marriages database and sends back a 'YES' response.

The identity checking process is then complete and the automated system activates Jack's pre-paid mobile phone account.

Jack's name and address information is provided by his CSP to the IPND Manager for inclusion in the IPND.

Later Jack checks with the university records and finds that his re-enrolment for the following academic year had not been correctly completed, thereby suspending his student details in the university database. Jack completed the re-enrolment process and sought confirmation that the university's electronic database now had him correctly identified as a current student.

CASE STUDY: CROSS-INDUSTRY ACCOUNT VERIFICATION SYSTEM (AVS)

Sanjay has owned his existing mobile phone on a post-paid payment plan for several years. To better manage his mobile phone expenditure, he goes into a CSP branded store to change his provider, his handset and his payment method.

The new CSP provides Sanjay with a new handset and pre-paid service, arranging for him to retain use of the mobile phone number he had been using.

While in the store, Sanjay provides his new CSP with his telephone number for his previous post-paid mobile service which was supplied by another CSP. The store assistant enters the identifying information into the telecommunications industry AVS interface on the store computer.

The AVS checks Sanjay's name, address and previous post-paid mobile telephone number with the account database records of his former CSP (which is also networked into the AVS) and provides a positive response.

The system registers that Sanjay's identity has been verified and his service can be activated as soon as his existing CSP completes the porting (transfer) of his number.

Sanjay's name and address information is provided by his CSP to the IPND Manager for inclusion in the IPND.

CASE STUDY: MANUAL VERIFICATION WITH EOI AUTHORITY

Maeve recently moved from New South Wales (NSW) to Victoria. She decides that she no longer needed a fixed service at her new house and instead purchases a pre-paid mobile phone from a convenience store.

She uses her new phone to call her CSP to activate the service, providing her name and new address details. She cannot provide her former landline number for checking against the data held in the AVS because the account had been in her flatmate's name. Instead, Maeve supplies her NSW driver licence details.

The operator informs Maeve that, with her permission, he could contact the NSW Roads and Traffic Authority to attempt to verify the driver's licence details or she could go into a retail shop of the CSP to show certain types of EOI document.

Maeve provides verbal (recorded) permission for the CSP operator to contact NSW Roads and Traffic Authority to check her details. The operator places Maeve on hold while he phones through to the Authority. The CSP and Authority operators consult and determine

that Maeve's driver's licence details are correct. The CSP advises Maeve that her details had been verified and her service is immediately activated.

Maeve's name and Victorian address information is supplied by the CSP to the IPND Manager for inclusion in the IPND.