Australian Communications Authority

The Secretary
Joint Standing Committee on Electoral Matters
Parliament House
CANBERRA ACT 2600

Dear Mr Chafer

I am pleased to enclose a written submission by the Law Enforcement Advisory Committee (LEAC) of the ACA to the Joint Standing Committee on Electoral Matters. The submission relates to the potential use of the electoral roll to facilitate identity verification in the sale of pre-paid mobile phone SIMs.

We appreciate the additional time that has been accorded to us to prepare this submission.

LEAC Members would also welcome the opportunity to provide oral evidence to supplement this submission.

Please do not hesitate to contact me on (03) 9963 6866 if you wish to discuss any matters relating to this submission.

Yours sincerely

Paul White
Chair, LEAC

4 April 2003

ABN 78 334 953 951
Level 13, 200 Queen Street, Melbourne, Victoria 3000
Telephone: (03) 9963 6800 Facsimile: (03) 9963 6899
TTY: (03) 9963 6948 Website: www.aca.gov.au
Postal Address: PO Box 13112 Law Courts, MELBOURNE VIC 8010

Submission from the ACA's Law Enforcement Advisory Committee on the potential use of the electoral roll to verify the identity of customers purchasing pre-paid mobile SIMs

1. The Law Enforcement Advisory Committee (LEAC) is a formal advisory committee to the Australian Communications Authority and is established pursuant to section 51 of the *Australian Communications Authority Act 1997*. It provides advice to the ACA on the law enforcement aspects of telecommunications regulation.

2. The LEAC has longstanding concerns that the abilities of carriage service providers[1] (CSPs) to accurately record and maintain the personal details of pre-paid mobile phone users is being undermined by identity fraud. The use of false identification or the provision of false personal details when purchasing pre-paid mobile phone SIMs (subscriber identity modules) can have serious, even criminal, consequences.[2] It can lead to further fraudulent activities being conducted, provide support to criminal activities, affect the investigatory capabilities of law enforcement agencies, and impede the ability of emergency service organisations to respond to emergency calls for assistance.

The identity verification requirements for pre-paid mobile SIMs

3. To try and address these problems, subordinate regulation in the form of the *Telecommunications (Service Provider—Identity Checks for Pre-Paid Public Mobile Telecommunications Services) Determination 2000* (the Determination) requires that identity checks are performed in association with the sale of pre-paid mobile SIMs.[3] Identity verification for post-paid services is not similarly regulated because the purchase of such services typically involve credit checks which also serve as a verification process.

4. The Determination provides for two alternative procedures that can be used, at the discretion of the CSP, to record and verify the identities of the purchasers of pre-paid mobile SIMs—a point-of-sale method and a post-sale method. These are explained in greater detail in Attachment B. In short, the point-of-sale method requires the retailers of pre-paid SIMs—who are typically not sections of the telecommunications industry—to sight and verify certain types of identification at the time of purchase. By contrast, the post-sale method allows purchases to be made without identification being sighted but instead involves the purchaser providing certain identifying information (eg. name, address, DOB, etc) to the CSP via a mandatory registration telephone call. The identity verification requirements apply only to the initial purchase of pre-paid SIMs, not to the re-charging of existing pre-paid mobile SIMs with additional credit.

---

[1] A CSP is defined in subsection 87(1) of the *Telecommunications Act 1997*. Persons are CSPs if they supply or propose to supply a listed carriage service(s) to the public using a network unit owned by a carrier. There are presently three CSPs that provide pre-paid mobile services, viz Optus, Telstra, and Vodafone.

[2] Background information about pre-paid SIMs is provided at Attachment A.

[3] The Determination is available on the ACA's website at http://www.aca.gov.au/legal/determin/telecom/simcard.htm and the accompanying explanatory statement at http://www.aca.gov.au/legal/determin/simcard/simcard_exp.htm

5. When the Determination was being developed in 1999–2000, it was intended that CSPs would employ post-sale verification processes to replace the point-of-sale arrangements which were being undermined by—and remain susceptible to—identity fraud.

The need for access to the electoral roll

6. To date CSPs have not been able to adopt the post-sale method due to the absence of an appropriate database facility or information resource against which the information that would be verbally provided by customers could be cross-checked and verified with sufficient confidence. A number of CSPs, in consultation with the ACA, have made concerted efforts in the past to examine whether there was a database solution that could be used for this purpose. Commercial database vendors have also been consulted to scope opportunities for the development of a dedicated database facility. However, database vendors consider that the post-sale verification method is not be feasible without access to a high integrity and comprehensive data source such as the electoral roll.

7. The electoral roll is considered by industry and the LEAC as the only reliable source of personal details of Australian citizens that provides a record of sufficient accuracy and integrity of the personal details of Australian citizens. Accordingly, this submission seeks the support of the JSCEM to enable those CSPs which provide pre-paid mobile services to utilise electronic access to the electoral roll for the purposes of a post-sale identity verification process, pursuant to the arrangements set out in the Determination.

How the electoral roll would be used

8. It is envisaged that the use of the electoral roll for this purpose would not involve 'disclosure' of the electoral roll content per se, but rather a more straightforward challenge/response arrangements. Information of a new customer would be entered into a secure interface at the CSP's end. The information would then be transmitted via a secure Virtual Private Network (VPN) tunnel and challenged against the database facility which utilised access to the electoral roll, amongst other information sources. A response would be received at the CSP's end advising that the data is either 'verified' or 'unverified'. In this way, access to the electoral roll content would be kept restricted to the absolute minimum necessary to achieve effective verification.

9. To date, the exploration of the potential use of the electoral has been limited given the existing restrictions on the use of the electoral roll under the *Commonwealth Electoral Act 1918*. However, the LEAC and its member CSPs would welcome the opportunity to explore the options for access in greater detail with the Australian Electoral Commission in consultation with database vendors.

Privacy would be protected

10. At the time of the introduction of amendments to the Privacy Act and related National Privacy Principles in December 2001, CSPs developed comprehensive in-house training systems to achieve compliance with all privacy requirements. It is envisaged that, to the extent necessary, this training would be extended to relevant CSP staff who would be involved with the verification process and use of

any database facility utilising electoral roll information. Comprehensive policies and procedures would also be developed to complement this training process.

11. Further, it is also envisaged that a condition of access to electoral roll data would be that the electoral roll would only be used for the purposes for which access has been granted—that is, for the verifying of the identities of pre-paid mobile SIM purchasers. Data is not intended to be downloadable from the database facility nor able to be viewed or searched by CSPs.

Concluding remarks

12. The LEAC recognises that the proposed use of the electoral roll is not a panacea for either identity fraud or the problems that can arise from the fraudulent misuse of pre-paid mobile SIMs. Sole reliance on the electoral roll would not provide a comprehensive solution to the verification of identification for all pre-paid mobile subscribers on a post-sale basis. For instance, such a solution would not be entirely 'foolproof' as there would still be potential for true information to be provided which did not relate to the user of the SIM or which was unable to be verified. (It is also not the intention to make enrolling to vote a de facto prerequisite for the purchase of a pre-paid mobile SIM.) Other sources of information would also be utilised in order to develop a robust solution that would cater for situations where electoral roll data would not meet (or be relevant to) identity verification requirements, such as in instances involving non-citizens, overseas visitors, and minors. Accordingly, access to the electoral roll is not seen as *the* solution but as an integral tool to be utilised as part of a broader set of solutions.

13. The LEAC appreciates that the electoral roll is neither established nor maintained for the purposes of identity verification or for the prevention of identity fraud. However, it is not unknown for the electoral roll to be allowed to be used for such purposes. For example, the Department of Family and Community Service is understood to have access to the electoral roll to aid in its detection and prevention of welfare payment fraud. Without access to the electoral roll, CSPs believe that the adoption of the post-sale process provided for in the Determination—similarly the development of the cross-checking facility on which it depends—will not be feasible. If CSPs are unable to adopt the post-sale process, they will be required to rely solely on the existing point-of-sale processes, the effectiveness of which is being undermined by the increasing problems associated with identity fraud.

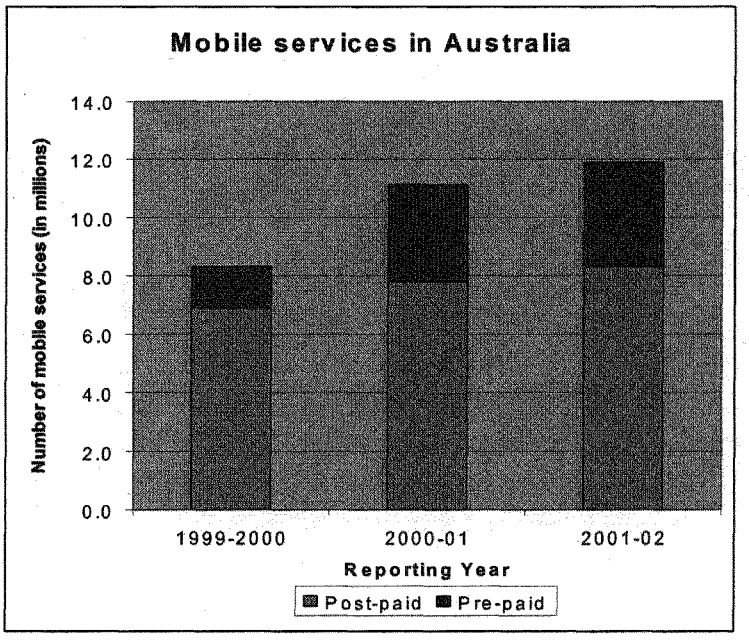
14. The LEAC would welcome the opportunity to discuss this matter in greater detail with the JSCEM.

Background information about pre-paid mobile phone SIMs

The SIM within a GSM mobile phone contains all the subscriber-related 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 calls to the emergency service numbers. CDMA mobile phones use different technology and do not (presently) utilise SIM technology.

Pre-paid mobile SIMs enable 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 on the user's pre-paid SIM. No further calls can be made once the pre-paid credit has been consumed (except to the emergency service numbers), although calls may still be received. The user then has the option of purchasing another pre-paid SIM (which may involve obtaining a new telephone number) or 're-charging' their existing pre-paid SIM through the purchase of further credit.

The alternative to pre-paying is post-paying, which typically involves a fixed-term contract with bills or tax invoices being sent to the customer at regular intervals in the same way as for fixed line phones. As shown in the graph below, approximately 3.6 million (or 30%) of the 11.9 million mobile services currently in operation are pre-paid. For the 2001–02 financial year, 31% of the 768,000 new mobile services were pre-paid. The number of pre-paid mobile services has increased from 1.4 million 1999–2000 to 3.6 million in 2001–02.



Pre-paid mobile SIMs can be purchased from an increasingly wide variety of retailers. Most of those retailers are not CSPs or telecommunications carriers under the *Telecommunications Act 1997*. Rather, they are authorised dealers or agents of CSPs. These dealers and agents commonly include:

- convenience stores;
- petrol stations;
- department stores;

- video rental libraries;
- electronics retailers (such as Dick Smith, Harvey Norman, and Tandy); and
- specialist retailers of mobile phones (such as Cellular One and Crazy John's).

Unlike carriers and CSPs, dealers and agents are not sections of the telecommunications industry and are therefore not within the jurisdiction of the ACA, nor subject to obligations under the Telecommunications Act or its subordinate regulations. Whereas the ACA is empowered under Telecommunications Act to enforce the compliance of CSPs with the Determination, the compliance of dealers and agents is governed through the CSPs' commercial contracts with their dealers and agents.

The Pre-paid SIM Determination

The point-of-sale identity verification method

The point-of-sale method requires the retailer to sight certain types of identification at the time of the purchase of the pre-paid mobile SIM.

If the purchase is made using cash or cheque, the point-of-sale method requires the retailer to sight—and to verify the sighting of—one 'Category A' document such as a driver's licence or passport; or two 'Category B' documents such as a bank card, telephone bill, or Medicare card. The acceptable Category A and B documents are listed in Schedule 2 to the Determination.

If the purchase is made using a credit card or debit card it is unnecessary to sight any additional identification documents as such cards, and the accounts behind them, warrant sufficient proof of identification.

Once the purchaser's identity has been recorded and verified, the sale is complete. However, as the pre-paid mobile SIM is sold in an inactive state, the customer must make a registration call to the CSP providing service for that product to request that the SIM be activated and enable access to the network.

All pre-paid products are currently sold using this point-of-sale method.

The post-sale identity verification method

The alternative method of registration provided for under the Determination allows CSPs to fulfil identity verification requirements at the time a new customer wishes to activate their SIM card for use.

This method of registration would allow a pre-paid mobile SIM to be purchased without the need to produce identification at the point-of-sale. The pre-paid SIM is sold to the subscriber in an inactive state. The subscriber must then make a registration call to the CSP providing service for that product in order to activate the service for the SIM and gain access to the network.

It is during that registration call that the identity verification requirements of the Determination would be addressed by the CSP. When the customer contacts the CSP for activation, the CSP will request certain identifying information to be provided pursuant to the Determination. If the identifying information is verified, the pre-paid SIM could then be activated for use by the customer. Under the Determination, the CSP would not be able to activate the SIM until that identifying information was provided and verified to achieve a total score of 30 points.

The acceptable identifying information, and the points value attributed to each, are listed in Schedule 3 to the Determination and include:

- full name (including second and any other names);
- residential, postal, and previous addresses;
- other telephone numbers;
- date of birth;
- employers name and address;
- passport reference number; and

- nearest cross street to the user's residential address.

Advantages of the post-sale method

The post-sale method has significant advantages over the point-of-sale method. It would centralise the collection and recording of pre-paid customer data with CSPs so that customers would only have to provide their details to CSPs during the registration call, rather than also providing that information to the retailer of the pre-paid mobile SIM. This is appropriate given that the customer's on-ongoing relationship is with the CSP and not the retailer of the SIM.

As mentioned above, the decision on whether to employ the point-of-sale method or the post-sale method is at the discretion of the individual CSP. Obviously though, if an efficient and effective post-sale method can be established, then it is likely to be a more attractive option for CSPs. Further, it is possible that CSPs may chose to utilise the point-of-sale method and the post-sale method for different sales channels. For example, the point-of-sale method might be retained for retail outlets controlled and managed by CSPs, while the post-sale method might be adopted for mass market sales channels such as those involving dealers and agents. Enabling CSPs to differentiate and self-regulate in this manner would ensure that identity verification obligations are satisfied in the most appropriate and efficient manner.

ATTACHMENT C

The identity verification requirements for pre-paid mobile SIMs in overseas jurisdictions

The LEAC understands that the identity verification requirements under the Determination are amongst the most comprehensive in the world. In most other countries, flexibility is afforded to the purchase and registration of pre-paid services. For instance, most European countries simply require identification of some sort to be produced at the time of purchase. In many cases information is not required or is not recorded or verified for subsequent retrieval to assist law enforcement agencies. There is also no subsequent attempt to ascertain the identity of the actual user of the service (as opposed to the purchaser of the SIM).

In New Zealand pre-paid mobile SIMs are sold in mass retail outlets in an activated state. A form is contained in the pre-paid pack that can be voluntarily filled out by subscribers and mailed back to the CSP. In this situation, free call credits are provided as an inducement to customers to voluntarily provide this information to the CSP.

Such processes are not as robust as the Australian process for collecting, recording and verifying information on pre-paid mobile customers.