New streamlined identity-checking requirements for prepaid mobile carriage services

ACMA Consultation on the Draft 2013 Determination - May 2013.

AMTA Submission – 11 June 2013

Background

The Australian Mobile Telecommunications Association (AMTA) is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile Carriage Service Providers (CSPs), handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry. For more details about AMTA, see http://www.amta.org.au.

AMTA has been an active participant in the Prepaid Working Group (PWG) convened by the Department of Broadband, Communications and the Digital Economy (DBCDE) and the Attorney-General's Department (AGD) and tasked with reviewing the regulatory arrangements for prepaid identity checks.

AMTA has also consulted closely with the Australian Communications and Media Authority (ACMA) as they have undertaken the process of drafting the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2013 (the new Determination).

AMTA recognises and appreciates the efforts of the ACMA, DBCDE and AGD in consulting with industry members.

Summary

In general, AMTA believes the draft Determination includes an activation based compliance process that adequately reflects the needs of consumers and meets the requirements of law enforcement and national security agencies (LENSAs).Despite the strong consultation process, however, industry remains fundamentally concerned with the direction of the regulatory process for the following reasons:

- Any regulation (current and proposed) requiring prepaid ID checks is an unreasonable burden on industry as no verification system yet proposed can guarantee the identity of every registered user. There is also no business requirement to verify customer ID for these services. The small number of individuals who wish to withhold their identity for criminal reasons will be easily able to do so even under the new system, while the vast majority of customers whose identity is verified accurately are of no interest to LENSAs.

- The proposed point-of-activation verification procedure utilising the DVS and other options represents an improvement on the current point-of-sale procedure because it increases flexibility. The proposal constitutes much less of an improvement if it replaces rather than complements the existing system. If identity must be verified for prepaid service users, the means should be as broad and varied as possible to ensure the least possible impact to CSPs and their customers.

- The proposed cost to CSPs of using the DVS to verify identity is high in comparison with the revenue associated with many prepaid services, which deliver far lower average revenue per service than postpaid services. In industry's view, DVS access costs should be borne

Government as the sole beneficiary of the procedure. If CSPs are required to pay these costs, some entirely legitimate low-cost business models may be rendered inoperable.

AMTA's members believe that higher levels of regulatory compliance can be achieved by CSPs in transitioning from a point of sale process to a process based on verification of customer evidence of identity at the point of service activation.

However, AMTA does not believe that the new Determination will ensure that users of mobile prepaid services are reliably identified, because:

- Prepaid mobile services are easily transferable between end-users;
- Stolen identity information can be used to verify identity (which actually provides an incentive for identity theft); and
- Prepaid mobile services can be imported from overseas.

The new Determination therefore remains a costly and burdensome regulation that is not likely to achieve its primary objective as set out in 2.1 (a).

AMTA notes that DBCDE's Regulatory Impact Statement states,

"*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*." [1]

Further, AMTA notes that based on the latest offering from AGD (May 2013), fees for accessing the Government's Document Verification Service (DVS) will be as follows:

Annual Volume	per calendar month	per query charge
< 400,000	<33,000	$1.40
>400,000 <600,000	>33,000 <50,000	$1.20
>600,000 <800,000	>50,000 <65,000	$1.00
>800,000 <1 million	>65,000 <85,000	$0.80
>1 million	>85,000	$0.65

[2]

An application fee of $5000 and a technical connection fee of $50 000 will also apply.[3]

Many mobile prepaid services are low cost and low margin services, sometimes sold for as little as $2 to $10 and with average revenue per user in the range of $15-30 per annum. The price of a DVS query and the cost of connection to the DVS for the mobile telecommunications industry must be proportionate to this or some business models will simply be unsustainable should industry be forced to absorb these costs.

[1] RIS p13
[2] Document Verification Service, Private Sector Access, National Service Offering, Industry Briefing Note, May 2013
[3] Ibid

While the new Determination provides CSPs with more options for compliance, both the existing and proposed new systems require customers to undergo a more complicated and invasive transaction than what would be required without regulation.

AMTA has made comments on the new Determination and issues raised in the ACMA's consultation paper below. AMTA has also commented on DBCDE's Regulatory Impact Statement in Attachment A.

New methods of identity verification as set out in the draft Determination 2013

Verification at point of activation – Part 5

In general AMTA supports the methods outlined in Part 5 and only notes the following concerns:

White listed email services

The verification transaction details should only consist of email address and not include IP address. IP addresses can be transitory and in some cases cannot be linked to an individual, in which case the verification transaction details will be unreliable. In other cases where the IP address can be linked to an individual, the recording of an IP address is unnecessary. Also the service activator should be required to give the CSP the "email address" rather than a "copy of the email address" as this wording is confusing and implies that the service activator must provide the CSP with a document.

Financial transactions

The rules set out in Item 4 of Schedule 4 are overly prescriptive in detailing how the CSP should handle the outcome of the nominal transaction. A CSP should, for example, be free to combine an amount debited from an activators financial account for verification purposes with debits made in relation to the service itself. Requiring the nominal verification amount to be refunded or reversed in all cases is inefficient and unnecessary.

Authorisation in Store

In discussions in the PWG, the objective was established that 99% of customers would be able to activate services over the phone or online and that less than 1% of customers would need to visit a store to complete activation. Even though 1% is a small proportion of customers, that still requires a process to be defined in the regulations for activation of services in-store. This has not been include in the draft determination, and needs to be. This process was defined in the PWG report by DBCDE.[4]

Authorisation by Community Leaders

The PWG report by DBCDE stated:

"The Working Group also took into consideration the needs of the various groups that rely on pre-paid services. Such groups may include people in remote and indigenous communities that may not have the required EOI. In such a situation, pre-paid services could be purchased by a community

[4] Prepaid Working Group, Proposal for Identity Verification for Prepaid Services at the Point of Activation, page 23

leader/elder or a community store who would keep a register of local consumers that would be available to LENSAs if required."[5]

AMTA requests clarification on how the ACMA intends to include consideration of the needs of people in remote and indigenous communities in the new Determination. Would the community leader/elder in such situations be regarded as a Carriage Service Intermediary?

Point of sale process – Part 4

AMTA believes that the new Determination should allow for current point of sale identity checks (in Part 4) to continue unchanged indefinitely and that this was the understanding of PWG members when agreement was reached on the original proposal for an activation-based process.

Any other option would mean that CSPs would be forced to transition to a point of activation process and in some cases this would mean CSPs would not be able to continue their operations. AMTA notes that many smaller CSPs have business models built around online sales where customers use credit/debit cards to purchase mobile prepaid services. It would seem most unreasonable to not allow a point of sale verification process to continue to be an option for such business models.

Similarly, for point of sale verifications where a credit/debit card is used to purchase the service, AMTA submits that CSPs should be able to visually check the credit/debit card details. If the details on the credit/debit card match the customer name provided, that should be sufficient verification without further need to either record the credit/debit card number or any transaction code on a paper or electronic form. AMTA received advice from the ACMA last year that a visual check of a credit/debit card was sufficient to satisfy compliance with the Determination. AMTA believes that capturing the transaction code adds no value as it is not unique and without knowing further details around the financial transaction (e.g. financial institution, type of account, time and date of the transaction, etc.) it is of no use.

If an obligation to record a transaction code is included in the new Determination, CSPs risk the vast majority of transactions using the current point of sale processes becoming non-compliant overnight. CSPs who wish to transition to the new activation based process may also have to take expensive and immediate action to revise compliance processes in order to meet the requirements of the new Determination to collect transaction details. CSP resources will be strained in achieving short term compliance with a new point of sale method and compliance to the long- term activation based method. The investment in achieving short term compliance will be stranded in a relatively short time.

AMTA notes the current AMTA point of sale forms used by many CSPs and approved by the ACMA have space for the recording of credit/debit card numbers and that the recording of credit/debit card numbers will be non-compliant under 7.3 (1)(b) of the new Determination. AMTA suggests that the ACMA work with industry to ensure that there is a reasonable grace period that allows for CSPs to inform retailers using the current forms of new obligations or to transition to the new activation based method.

[5] Prepaid Working Group, Proposal for Identity Verification for Pre-Paid Services at the Point of Activation, Page 11

AMTA notes that in the case of online purchases a transaction code is likely to be recorded and easily associated with the mobile number by the CSP whereas in a storefront setting a transaction code recorded on a paper or electronic form will not be traceable when a CSP has multiple retail outlets. In this case there may be no recorded retailer to connect the transaction code with the actual transaction details.

AMTA also requests that the new Determination provide clarification on the use of new e-commerce payment platforms for online purchases such as PayPal, eWay and Paymate. In particular, whether recording the transaction code would be sufficient for these types of payments.

Provisional activations

AMTA considers that the inclusion of provision in the new Determination to allow for provisional activations in certain circumstances is in the best interests of our members' customers and is critical for a workable solution.

Implications for customers

AMTA's first priority is to take into consideration the impact the proposal will have on the customers of our members. Provisional activation processes should deliver a fair and reasonable outcome for consumers who have purchased a prepaid service and have a reasonable expectation to be able to use it straight away. There are two scenarios in which a provisional activation should be allowed.

1. DVS unavailable

If the DVS is off-line or experiences an unscheduled failure, customers should not be disadvantaged by being prevented from using a service they have legitimately purchased. Law enforcement and national security agencies have represented that it is absolutely critical that CSPs be able to perform ID checks. It therefore follows that CSPs should be able to rely on an appropriate level of DVS availability. If the DVS availability is not commensurate with such a standard, then provisional activations, within limits, are a reasonable expectation for both industry and consumers. AMTA notes that DVS service levels are yet to be confirmed.

AMTA submits that it is reasonable to provide customers and CSPs with a provisional activation capability in instances where the DVS or source databases are off-line or experience unscheduled failures. AMTA also submits that CSPs would be able to verify such provisional activations within a reasonable timeframe of the DVS coming back online.

2. Financial transaction

AMTA also notes that the financial transaction activation check, as per Part 5, is reliant on being able to have confirmation of the transaction sent back to the service provider. This option was developed by the PWG with the full understanding that with some transaction methods (e.g. BPAY on direct debit bank transactions) there is a delay between the time the transaction is processed and the time confirmation of the transaction is provided back to the retailer. Without the ability to provide a provisional activation in these circumstances, the financial transaction method is essentially invalidated as an option. For this reason, AMTA considers that provisional activations should be available in these circumstances.

AMTA acknowledges that for a workable provisional activation solution there needs to be appropriate protocols in place to address the situation where a customer has been provided with a provisional activation in which the transaction/DVS check is later rejected. In these circumstances, AMTA considers it would be appropriate that the service would be suspended pending the customer satisfying the requirements of the new Determination.

The decision on provisional activation is a balance between the impact of prepaid services being activated by persons without undertaking relevant ID checks and the impact on customers who are unable to use a service they have paid for due to circumstance beyond their control. AMTA considers that the impact on customer satisfaction is clear. What is less clear is the benefit of persons of interest manipulating this process to activate a service without an ID check (noting that the service would be suspended once a check has been invalidated) and the consequential impact on law enforcement. AMTA therefore considers that, on balance, provisional activations should be provided for in the new Determination.

Exemptions in cases of emergency or natural disaster – Part 3

AMTA notes that in emergency situations and natural disasters mobile providers have consistently demonstrated their credentials as good corporate citizens and provided assistance to people as needed. Continued ability to supply such assistance is essential.

Further, the mobile industry must be able to provide such assistance within a flexible and reasonable regulatory framework that appropriately balances the communications needs of people affected by an emergency or disaster against the low risk of abuse by persons intending to deliberately conceal their true identity.

Responses during natural disasters and emergencies tends to be driven primarily from front –line staff and imposing additional administrative activity will likely substantially increase the risk that the process will be ignored or, that members of the community, already suffering hardship, will be unable to access services at a time when telecommunications are vital to restoring their lives .

AMTA therefore supports the inclusion of an exemption in cases of emergency and natural disaster as set out in Part 3 as it both meets the needs of affected communities and encourages compliance.

AMTA also suggests the following changes to the current drafting in Part 3:

Threshold for Emergency in 3.1(a)

AMTA understands that the intent of linking this process to an 'emergency' as defined in 275C of the *Telecommunications Act 1997*, was to ensure that this process was not abused by spurious claims as a means of avoiding compliance obligations. However, AMTA is concerned that there may be smaller localised events where there are consumers who are equally worthy of emergency assistance but where those events do not reach the threshold of an "emergency" as defined under the Act.

Therefore, AMTA suggests that it is in the public interest to include a capacity for CSPs to notify the ACMA of emergencies and provide details of the event and allow the ACMA to exercise its discretion to enable CSPs to provide assistance and emergency relief.

Timing of distribution of the end-user equipment

The drafting in clause 3.1(2)(a) appears to assume un-activated services are distributed. AMTA also submits that in 3.1 (2)(a) it is unclear as to whether the 7 day period starts to run from the date of the disaster first occurring or the date that the disaster is declared an 'emergency' as per clause 275C of the Telecommunications Act 1997. AMTA suggests that this clause is amended so that where a service has been pre-activated; no time limit is applied to the distribution of the service.

The operation of clause 3.1 (2)(c) places a 30 day time limit on how long a service may remain active. As a result, placing a time limit on the date of distribution of a pre-activated service is not relevant. For example, if the service was pre-activated on day 1, whether or not the service was distributed on day 7 or day 8 is irrelevant, as the service would still need to be cancelled on day 30.

Exempt individual

AMTA suggests that the definition of an 'exempt individual' could be simplified to refer to an individual who has been directly impacted by a natural disaster or emergency as this would cover those who are affected while staying somewhere other than their principal residence e.g. holidaymakers caught in bushfires or storms.

Record-keeping requirements in Part 7

As discussed above in relation to Part 4 point of sale processes, AMTA believes that, excluding online purchase transactions, it would not be useful to require CSPs to record a 'transaction code' in the case of purchases using a credit or debit card.

AMTA believes that the current point of sale process (as approved by the ACMA) that allows CSPs (or their agents) to perform a visual check of the credit/debit card to ensure that the name matches the customer name provided is sufficient. All that should be required to be recorded is that the purchase was made by credit/debit card.

AMTA also requests amendment of the requirement regarding records in 7.3. CSP IT systems will necessarily have to record, even if temporarily, the identifying number of a government document or a credit/debit card number in order to process the transaction or query the DVS, particularly where the DVS may not be available at the time of the service activation. AMTA notes that *the Acts Interpretation Act 1901* states at section 25:

> ***25 References to writing, documents and records***
>
> *In any Act, unless the contrary intention appears:*
>
> ***document** includes:*
> *(a) any paper or other material on which there is writing;*
> *(b) any paper or other material on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them; and*
> *(c) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device.*
>
> ***record** includes information stored or recorded by means of a computer.*
> ***writing** includes any mode of representing or reproducing words, figures, drawings or symbols in a visible form.*

AMTA's view is that the *Acts Interpretation Act* applies to subordinate legislation and that services providers will be creating a record for any information entered into their IT systems. AMTA considers that the intent of the requirement in 7.3 could be met by amendment to:

(a) keep an enduring record of the identifying number of a government document; or
(b) keep an enduring record of a credit or debit card number.

Requirement to keep a written description of compliance arrangements

AMTA supports this requirement.

AMTA believes that Part 5 of the new Determination that allows CSPs to access the DVS as part of their service activation process will provide sufficient means of document validation to enable most customers to submit evidence of identity details and enable activation of their service without having to visit a store.

By implementing an activation system and processes that includes verification by the DVS a CSP can achieve compliance with the Determination by building additional steps into its operational and customer service systems.

AMTA believes that a service provider that puts in place appropriate IT systems and operational processes, with appropriate checks and balances as well as adequate staff training, should be confident that they have minimised compliance risks. AMTA requests inclusion of a further division in Part 5 as follows:

Division 5.4 Compliance

5.6 A carriage service provider that has established reasonable processes, policies and procedures to meet the requirements of Divisions 5.2 and 5.3 and Part 7 will have met its obligation to comply with this Determination.

Drafting comments

Definition of Prepaid Mobile Carriage Services

AMTA believes that the definition of prepaid mobile services still leaves open the compliance risk that month by month services supplied on a contract will be regarded as prepaid where the customer pays in advance and makes no additional payment for the service. Compliance requirements will be driven by customer usage and payment history and not by the fundamental nature of the plan type. Further work on the definition is required so that the scope of the Determination is not beyond the intended mobile service type. Points (a), (b) and (c) in the definition apply as much to post paid services as they do for prepaid services and thus add nothing to the distinction between the two. Point (d) is written in terms of an individual customer payment in a manner that does not sufficiently distinguish between prepaid and post paid contract arrangements.

Object of Determination

AMTA suggests that Points (a) and (c) in 2.1 should be changed to read “identify purchasers or service activators” in order to be consistent with section 2.3.

Authentic, Accurate and Up to Date

The objective of identity verification processes is to validate that the identification information supplied currently exists. AMTA suggests that Section 5.5 and Schedule 4 could be simplified.

The text in 5.5 could more simply read:

“The carriage service provider must, using one of the methods specified in column B of Schedule 4, verify the identifying evidence supplied by the customer.”

Text in Schedule 4 could be amended to read:

“…the carriage service provider is taken to have verified the identifying evidence if:”

Attachment A: Comments on the Regulatory Impact Statement

1. AMTA recognises that the new Determination will provide more options and flexibility in terms of compliance for CSPs and therefore supports it.

2. AMTA also notes that the new Determination gives CSPs a practicable method to comply with their requirements by enabling systemic compliance to be built into the CSPs activation processes.

3. AMTA notes that the costs of accessing the DVS combined with the capital costs of system and IT changes required to connect to the DVS as well as costs of implementing changed processes throughout the CSP's supply channels will be critical in determining if the DVS approach is economically feasible.

4. The Productivity Commission noted in its 2012 Report on its Annual Review of Regulatory Burdens on Business that the review of the regulations should examine:

   "…*whether the cost of verifying identity and collecting data should be borne by law enforcement agencies or the government, as the data is being collected for public benefit*."(p153)

   Despite this matter being raised on several occasions in both the PWG and the Experts Group, no substantive review of cost-sharing arrangements has been undertaken. Industry members firmly believe that LENSAs should directly bear the identifiable costs of the regulation that exists solely based on their requirements and which provides no benefit to industry.

   In particular, AMTA considers that it would be fair and reasonable to make DVS queries free of charge to CSPs as CSPs have no business requirement to make a DVS query. A regulatory burden is being imposed that will also potentially generate revenue for another arm of Government if the costs of DVS queries are not recoverable by CSPs as provision of assistance to law enforcement agencies.

5. Many mobile prepaid services are low cost and low margin services, sometimes sold for as little as $2 to $10 and with average revenue per user in the range of $15-30 per annum. The price of a DVS query for the mobile telecommunications industry must be proportionate to this or some business models will simply be unsustainable should industry be forced to absorb these costs.

6. A proper cost-benefit analysis has not been undertaken as law enforcement and security agencies have not quantified the perceived benefits of the regulation of identity checks for mobile prepaid services. AMTA notes that the justification for the regulatory burden being imposed is declarative in nature and is not evidence-based.

7. Further, the advice from law enforcement agencies appears to be contradictory in that agencies are concerned that the current process is providing little or no benefit but also claiming that if the existing regulation was not in place that it would result in a "serious reduction in capability" for agencies.

8. AMTA notes that there is no business case for CSPs to undertake identity checks for mobile prepaid services and that the cost burden imposed on industry by this regulatory requirement (that cannot actually verify a customer's identity; only that a form of ID presented is valid) has the potential to be in the order of millions of dollars.

9. Further, Government has not engaged with industry on the issue of cost recovery for the provision of assistance to law enforcement and security agencies by use of the DVS. The RIS ignores the capital costs that will necessarily be incurred by CSPs in developing a point of activation-based verification system.

10. AMTA notes that industry was not consulted during the development of the cost analysis included in the RIS. AMTA considers this to be an unusual omission given the in-depth consultation on all other elements. Further, industry estimates of the costs of the current system have been used as the basis for comparison to DBCDE estimates of costs of the proposed system. A more transparent 'like for like' analysis should have included industry estimates of what the proposed system will cost industry, rather than rely on DBCDE estimates.

11. AMTA believes that a review after only two years would be premature as connection to the DVS and implementation of system changes will likely take between 12-24 months. A review after only two years would not adequately assess change. AMTA suggests that four years would be a more appropriate timeframe for a review.

12. If a review is undertaken it should quantify the costs that industry incurs, including implementation costs, against the corresponding number of queries by law enforcement agencies on prepaid services over the same period. This would provide greater transparency of the cost of delivering a customer ID verification at the point of activation of a mobile prepaid service.

13. Further, AMTA does not believe that the current point of sale arrangements should be considered for removal. AMTA believes that the new Determination should allow for current point of sale identity checks (in Part 4) to continue unchanged indefinitely and that this was the understanding of PWG members when agreement was reached on the original proposal for an activation-based process. Any other option would mean that CSPs would be forced to transition to a point of activation process and in many cases this would mean CSPs would not be able to continue their operations. AMTA notes that many smaller CSPs have business models built around online sales where customers use credit/debit cards to purchase mobile prepaid services. It is unreasonable to not allow a point of sale verification process to continue to be an option for such CSPs.