



Emergency Call Service Determination

Proposed amendments to ensure mobile phones can access the Triple Zero (000) emergency call service

Public submission

9 October 2024

Executive Summary

Telstra welcomes the opportunity to respond to the Australian Communications and Media Authority (ACMA's) consultation on Emergency Call Service Determination (ECSD): Proposed amendments to ensure mobile phones can access the Triple Zero (000) emergency call service (the "**Consultation**") and the Draft Telecommunications (Emergency Call Service) Amendment Determination 2024 (No. 1) ("**Amendment Determination**"). We support the Minister's goal to give consumers increased confidence that their devices are capable of making emergency calls.

We note the ACMA is seeking to address two issues simultaneously with this amendment: 1) addressing the near-term problem of devices that will not be able to make emergency calls after the closure of the remaining 3G networks, and 2) facilitating a longer-term solution to better manage the emergency calling capability of future devices and network evolutions. We recommend decoupling these goals so the ACMA and industry can initially focus on finalising the requirements for the closure of Australia's two remaining 3G networks on 28 October 2024. We suggest the longer-term solution be finalised as part of the ACMA's next consultation on amendments to the ECSD to give effect to the "Bean Review" recommendations that are to be implemented by 1 April 2025.

While we support the overall draft amendments to the ECSD, our submission recommends five minor changes to the wording in the draft Amendment.

- **Recommendation 1:** Change the language in the Amendment Determination from "*not supply a service*" to language such as "*deny the mobile phone access to the service*", or "*prevent the mobile phone from accessing the service*". This will allow Mobile Network Operators (MNOs) to block the devices from accessing the network. This will provide a **better experience for consumers** as they will have immediate access to a working service after transferring a SIM from a blocked device to one that is not blocked.
- **Recommendation 2:** Change the language in the Amendment Determination from "*identify whether a mobile phone can access the emergency call before supplying a service*" to "*as soon as the MNO becomes aware ...*". This is because it is not possible to identify the device **before** it has attached to the network.
- **Recommendation 3:** If the ACMA is not minded to adopt Recommendation 1, the language in the Amendment Determination should be changed to allow MNOs the option to restrict access to only the Standard Telephone Service (STS). This would allow data and text (SMS) carriage services to remain operational, while denying all network-based voice calls. It would also allow customers some means of communication (e.g., text message or voice calls through over-the-top apps such as WhatsApp or Messenger) so they could contact family members or friends for assistance.
- **Recommendation 4:** We recommend a note is inserted at the end of sections 62 and 64 of the Draft Amendment Determination to the effect: "*Note: A device is considered to be capable of making an emergency call if it can make an emergency call on any of the 3GPP bands offered by the relevant Carrier that the device also uses to make normal voice calls.*" This will have the effect of exempting devices that do not support 3GPP Band 28 (700 MHz) but are otherwise compatible with the other 3GPP bands used in Australia.
- **Recommendation 5:** The ACMA should include a definition of "Mobile Phone" in the Amendment Determination, to avoid ambiguity on the type of device that is required to be denied access to a carriage service(s).

[CIC Begins]

[CIC Ends]

It is also not possible for us to unambiguously distinguish between a foreign traveller acquiring a local service (e.g., prepaid SIM) any other resident Australian purchasing a prepaid SIM, and so we will not be



able to provide the benefit to our customers from the exception proposed for foreign travellers in section 67.

We conclude our submission by explaining the mechanism we plan to deploy on 28 October. We have also answered the ACMA's 24 consultation questions.

Contents

Executive Summary	2
1 Introduction.....	5
2 Concerns about drafting in the Amendment Determination	6
2.1 “Device” rather than “Service”	6
2.2 Device type is not known until the device attaches to the network.....	7
2.3 Option for only Standard Telephone Service, rather than all Carriage Services	7
2.4 Non-Band 28 devices should not be denied access (should be out-of-scope)	8
2.5 A definition is required for a mobile phone	9
3 [CIC Begins] [CIC Ends]	10
3.1 There are limitations to supplying notification(s) once a device is blocked	10
3.2 [CIC Begins] [CIC Ends].....	10
3.3 We cannot utilise (give effect to) the exception for foreign travellers (s.67)	10
4 Telstra’s approach to device blocking after 28 October 2024	11
Appendix 1: Answers to the ACMA’s consultation questions	12

1 Introduction

Telstra welcomes the opportunity to respond to the Australian Communications and Media Authority (ACMA's) consultation on Emergency Call Service Determination: Proposed amendments to ensure mobile phones can access the Triple Zero (000) emergency call service (the **Consultation**).

In August 2024, the Minister for Communications directed¹ the ACMA to amend the ECS Determination (ECSD) to improve the reliability of access to the Triple Zero ECS in response to the recommendations from the Bean Report and the shutdown of the 3G mobile networks. We support the Minister's goal to improve consumer confidence that the devices being used by consumers are capable of making emergency calls. This is an important goal, given the plethora of mobile phones (handsets) currently in operation in Australia. Some of these phones are designed or configured to operate in countries other than Australia, and while most devices configured for other countries can make emergency calls on Australian mobile networks, this is by no means guaranteed. The ability to make emergency calls is a critical function for a mobile phone, and many of the phones designed for overseas markets are not tested for Australian networks. Tightening up the supply arrangements for devices, especially for emergency calling capability, and updating and enforcing **minimum device compliance regulation** will reduce future risk of a consumer having a device that is not capable of making an emergency call in Australia.

We also appreciate that the ACMA is attempting to deliver two goals simultaneously with this amendment: 1) addressing the near-term problem of devices that will not be able to make emergency calls after the closure of the two remaining 3G networks in Australia; and 2) facilitating a longer-term solution to manage future devices and future network evolution (e.g., the future closure of 4G networks) arising from the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) review into the Optus outage of 8 November 2023 (the "Bean Review").

We support both goals but are concerned that attempting to deliver both simultaneously is challenging given resource constraints and the tight timeline to settle the changes to the ECSD. We think it would be prudent to initially deal with the devices impacted by the 3G network closures, then tackle the second goal after the 3G networks are closed. Separating the two goals in this manner reduces the risk of further delay to 3G closure (which has now been delayed twice for Telstra), and avoids "rushing" development of the longer-term, strategic solution. We suggest the longer-term solution be finalised as part of the ACMA's next consultation on further ECSD amendments to address the other "Bean Review" recommendations that are to be implemented by 1 April 2025.

With all this in mind, our submission recommends five minor changes to the wording in the draft Amendment to make the determination effective. **[CIC Begins]**

[CIC Ends] Our submission is structured as follows:

- Section 2 provides commentary on the drafting of the Amendment Determination, and explains the five minor changes we require to be able to minimally comply with most parts of the proposed amendments;
- Section 3 **[CIC Begins]**

[CIC Ends]

- Section 4 contains a short "explainer" on the mechanism we plan to deploy to give effect to the proposed Amendments; and
- Appendix 1 contains specific answers to each of the ACMA's twenty-four consultation questions.

¹ Australian Communications and Media Authority (Emergency Call Service Determination) Direction 2024, available at: <https://www.legislation.gov.au/F2024L01103/asmade/text>

2 Concerns about drafting in the Amendment Determination

In this section, we describe our concerns with the drafting of the Amendment Determination. As outlined in the introduction, we are looking at the drafting with a focus on the near-term goal of closing the remaining two 3G networks on 28 October in a manner which minimises the risk of customers being unable to make emergency calls after that date.

We agree with, and support, the longer-term goal of creating a robust device standards environment, that includes denying access to carriage services for devices that do not comply with the standards we set, including standards for emergency calling capability. However, the immediate goal is to put in place a mechanism that removes access to the three public mobile networks for devices that will not be able to make emergency calls post 3G-closure. This must be the primary focus for the Amendment Determination.

2.1 “Device” rather than “Service”

The draft Amendment Determination requires CSPs to not supply a **service** (s.62, “*Before supplying a service to a customer...*”) or not supply a **carriage service** (s.63(2)(b) “*not supply carriage services to the customer...*” and s.65(4) “*... cease to supply any carriage services ...*”). There are two different ways to achieve this. 1) Deactivate or suspend “the service”, or 2) deny access (i.e., prevent entry) by “the device”.

At first, it might appear academic or a matter of semantics as to how the legislation is written, because preventing the device from accessing the network does *give effect* to the obligation to cease supplying the service. Nevertheless, we recommend it is better to describe the course of action to be taken in reference to the “device” rather than the “service”. This is because it is the *device* (not the network) that is not capable of placing the emergency call, for example because the device does not support VoLTE emergency calling (it can only make emergency calls over 3G).

Additionally, describing the course of action in terms of “the device” is also important, because if denial occurs at the service level (as per the current drafting), there are two problematic consequences:

- Deactivation or suspension of “the service” then requires the service to be reactivated once the end user has obtained a replacement phone. In practice what this means is the end user will need to contact their service provider, which they cannot do using either their old or their new phone because the service is deactivated. This is not an acceptable customer experience and creates a frustrating customer journey. If, however, “the device” is denied access to the network (blocked), then the instant the end user inserts their existing SIM, or transfers their eSIM to a new device, they are fully operational. No further action is required by either the customer or service provider.
- Where the service is supplied to the customer by an MVNO, the MNO may not have the legal right or technical ability to suspend/deactivate “the service”; only the MVNO can. This is because the MVNO is in control of “the service” through their customer management systems. In addition (as explained in section 2.2), it is not possible to know what mobile phone the customer intends to use in advance of the phone attaching to a mobile network. Only the MNO (network operator) will be able to identify the mobile phone, and even then, only after the mobile phone has attached to the network. Thus, if it is “the service” that is to be deactivated or suspended, firstly, the MNO will need to detect and identify the mobile phone the end user is using, and then inform the MVNO that the mobile phone is not capable of an emergency call, so the MVNO can then suspend/deactivate “the service”. There are no IT systems in place to automate the transfer of such information, and it would not be possible to build such systems (which requires changes to existing APIs to contain the new information and for the MVNOs to update their systems to utilise this information) by 28 October 2024, and not for some considerable time after that date. For now, information can only be supplied from the MNO to the MVNO on a manual, ad hoc basis.

These two limitations mean that if the ECSD is amended to require CSPs to not supply a service, this will trigger convoluted processes for consumers, and between MNOs and MVNOs. This will lead to poor

customer experience, and inconsistent implementation of the obligations in an amended ECSD (for example, depending on the timing of ad hoc updates between the different MNOs and MVNOs, some end users may experience a short delay between using a device that is to be denied access to a service and that service being cut off, whereas other end users may enjoy a much longer period of time).

Recommendation 1: We recommend the language in the Amendment Determination is changed from “not *supply* a service” to language such as “*deny the mobile phone access* to the service” or “*prevent the mobile phone from accessing* the service”.

It is worth noting that our proposed language still allows a CSP (MVNO) or MNO to give effect to the obligation by suspending or deactivating the service (should they so choose), as suspension/deactivation would also have the effect of not allowing the user to access the service. The benefit of the change we are proposing, is that it supports MNOs giving effect to the obligation by *blocking the device*.

2.2 Device type is not known until the device attaches to the network

The draft amendment requires CSPs to “... *identify whether a mobile phone can access the emergency call service before supplying a service*.”² [emphasis added]. In other words, the current drafting requires the CSP to know what device the customer plans to use before the CSP is permitted to supply a carriage service to the customer. This is simply not possible. Many customers are Bring-Your-Own-Device (BYOD), and until such time as the device attaches to the network, there is simply no visibility of the device the end customer intends to use.

Further, it is not a simple task to “ask” the customer at the point of sale (including online channels) what device they’re planning to use. It is insufficient to ask the customer for a make and model (e.g., Apple iPhone 5), because within a given make/model of mobile phone, there can be customisations for different countries. An Australian variant of a make/model may be fine, whereas an American one may not. To avoid inadvertently denying access to tens or even hundreds of thousands of mobile phones, it is necessary to know the Type Allocation Code (TAC)³ for the device, and this can only readily be identified after the device attaches to a network. Considering the range of MVNOs, spanning purely online retailers to supermarket chains, imagine an assistant at a supermarket trying to help someone who is less technically literate obtain the TAC from their device, so the assistant can determine whether or not to supply a service.

Recommendation 2: We recommend the language in the Amendment Determination is changed from “*identify whether a mobile phone can access the emergency call before supplying a service*” to “**as soon as the MNO becomes aware** a mobile phone cannot access the emergency call, *deny access to the service*” (or “*to the carriage service(s)*”).

Note: our recommended change refers to “the MNO” and not “the CSP”, as only the MNO can detect the device.

2.3 Option for only Standard Telephone Service, rather than all Carriage Services

If the Amendment is changed, as we recommend in section 2.1 to focus on “devices” rather than the “service”, this section of our submission is moot, because denying access to the entire device means it cannot access any carriage services (i.e., blocked from *all* carriage services), in which case, this section can be ignored.

² Section heading for s.62

³ The Type Allocation Code (TAC) is a unique code identifying the make and model of the device. Using the TAC, an MNO can look up the capabilities of the device (mobile generations supported, 3GPP bands supported, etc) in a database such as the GSMA TAC database. See <https://www.gsma.com/solutions-and-impact/industry-services/device-services/gsma-device-attribute> for more details.

65% of the land mass not covered, there are many places you can go where there is no coverage, even with a device that supports every band in Australia.

Devices that do not support 3GPP Band 28 simply reduce the area where the consumer has coverage. Some consumers will be happy with that arrangement, because they do not regularly venture into the bush or rural areas where they're likely to encounter limited coverage. As such, we see no reason to block these devices from accessing the network.

We therefore propose that devices which do not support 3GPP Band 28 be considered outside the scope of this instrument (i.e., these devices do not need to be denied access to a carriage service), because they have no issue making an emergency call (the device is completely capable of making an emergency call on the bands that the support), and while there are locations where the device will receive "no signal", this is already a common occurrence, given any device will experience "no signal" for 65% of Australia's landmass.

Recommendation 4: A note is inserted at the end of sections 62 and 64 of the Amendment Determination to the effect: *"Note: A device is considered to be capable of making an emergency call if it can make an emergency call on any of the 3GPP bands offered by the relevant Carrier that the device also uses to make normal voice calls."*

2.5 A definition is required for a mobile phone

The proposed Amendment Determination refers, in several places, to a "Mobile Phone", however, the term "Mobile Phone" is not defined in the definitions. We consider it important that a definition is added, to avoid ambiguity of the type of device that is intended to be captured by the Amendment.

A "phone", mobile or otherwise, is commonly perceived as a device capable of making a voice call across a network. Cars being manufactured today often come with an embedded SIM, and the higher-end cars include a concierge service for support from everything from directions to break-down support. People speak of their car "having a phone in it", because it can make a voice call to the concierge. Similarly, people may describe a SmartWatch or a tablet as having a phone in it, if it can make a voice call.

We understand the intent of the Government is to only capture devices that are a handset form-factor, such as Smart-Phones, flip-phones, push-button phones, etc. We consider it is insufficient to simply rely on the "ordinary meaning" (as posed in consultation question 2) of mobile phone to define the range of devices that are in scope, or more importantly, exclude device types that are out-of-scope.

Additionally, some mobile devices maybe used for purely business services, for example scanning stock in a warehouse. While these devices could technically make phone calls, they are not used to make phone calls, and are not used to make emergency calls. If these devices were blocked it would create a substantial and unnecessary business impact and cost. Therefore, we recommend that machine to machine and Internet of Things use cases are excluded from the Amendment Determination.

Recommendation 5: The ACMA should include a definition of "Mobile Phone" in the Amendment Determination, to the effect of: **mobile phone** means a device that is a handset form-factor, and is used, or is capable of being used, in connection with a Standard Telephone Service (STS) over a public mobile telecommunications service (PMTS), excluding devices which are primarily used for Machine to Machine or Internet of Things use cases.

[CIC Begins]

[CIC Ends]

3.1 There are limitations to supplying notification(s) once a device is blocked

Once a device is denied access to a carriage service (i.e., blocked, see section 2.1) then it is no longer possible to send text messages or Recorded Voice Announcements (RVAs) to that customer. This means the CSP must rely on ancillary methods (email, post, information on a website) to communicate with the customer after the customer's device has been denied access.

We appreciate the draft Amendment Determination does not specify the form the notification must take,⁹ and therefore, notifications via email or post meet the requirements of the proposed amendment, i.e., the obligation does not require the notification go *to the device*. However, we do not always have email address details (or the details are not current), nor do we always have postal details.

As such, we note that we may not be able to comply with the requirements in sections 63(2)(a), 63(2)(c), 65(2)(a)-(d) and 65(3), in each instance, as blocking cuts off our ability to communicate with the device directly, and in some cases, we do not have alternative contact details.

[CIC Begins]

[CIC Ends]

3.3 We cannot utilise (give effect to) the exception for foreign travellers (s.67)

In our proposed solution (see section 4), it is not possible to unambiguously identify international travellers arriving in Australia with a mobile phone that we know is unable to make emergency calls from Australian residents. While we do know when foreign travellers are using *international roaming*, this is not the only method under which foreign travellers appear on mobile networks in Australia. In order to avoid high international roaming charges, foreign travellers to Australia often purchase a prepaid SIM upon arrival (indeed, there are vending machines at airports specifically to meet this demand), however, it is not possible to accurately determine whether the person purchasing a prepaid SIM is a foreign traveller or a local resident.

In addition, our proposed solution, which denies access to a mobile network by blocking the device (see section 4), means that it is not possible for us to give foreign travellers who use international roaming an exception, as the blocking mechanism is completely unaware of the cohort the end user may belong to. Anyone, regardless of who they are, will have their device blocked if it is known to be unable to make an emergency call on the provider's own network, or the device is known to be unable to camp-on to another network.

⁹ Sections 63(2)(a), 63(2)(c), 65(2)(a)-(d) and 65(3).

4 Telstra's approach to device blocking after 28 October 2024

This section provides a brief “explainer” on the mechanism we will use from 28 October 2024 onwards to deny access to a carriage service to mobile phones identified as not being able to place an emergency call either on the provider's own network or to emergency camp-on to another network. For clarity, the mechanism we propose is purely the mechanism we are proposing for our network; not for consideration by any other mobile network operator in Australia.

Telstra proposes to use a network-based mechanism that determines the Type Allocation Code (TAC)¹⁰ of the mobile phone and checks to see if that TAC is on our “blacklist” of TACs. The “blacklist” is a list of devices we know are either unable, or will become unable (once the remaining 3G networks are closed) to make an emergency call directly on our network, or by camping-on to another network.

If the TAC is on the blacklist, the mobile phone is denied access to the network.¹¹ The TAC can be obtained from the International Mobile Equipment Identifier (IMEI)¹² of the mobile phone when the mobile phone attempts to attach (i.e., “log on”) to the network. The IMEI is a unique “serial number” to every mobile device, including IoT devices and other non-mobile phone devices. Importantly, where the TAC is on our “blacklist”, the mobile phone is immediately denied access to the network. In other words, the “log on” process is stopped, the mobile phone is denied access, and will simply display “no service” (or similar). At this point, no further communication is possible, either to or from the mobile phone. It is not possible to send/receive text messages, voice calls, or data.

As noted in section 0, there are limitations to the TAC blocking approach, as it is not possible to differentiate between different user cohorts, such as foreign travellers, or existing versus new services.

We are able to deploy this solution on 28 October 2024, such that we will be able to commence denying network access to customers with a mobile phone that cannot make emergency calls access from the date we will shut down our 3G network.

¹⁰ The Type Allocation Code (TAC) is a unique code identifying the make and model of the device. Using the TAC, an MNO can look up the capabilities of the device (mobile generations supported, 3GPP bands supported, etc) in a database such as the GSMA TAC database. See <https://www.gsma.com/solutions-and-impact/industry-services/device-services/gsma-device-attribute> for more details.

¹¹ For clarity, mobile phones that are denied access to the network using this blocking mechanism, are ordinarily still able to make emergency calls, as the denial of access contains an exemption for emergency calls. Of course, the mobile phone targeted by this Amendment are specifically those devices that are not, or will not, be able to make emergency calls once the remaining 3G networks in Australia are closed on 28 Oct 2024.

¹² See https://en.wikipedia.org/wiki/International_Mobile_Equipment_Identity

Appendix 1: Answers to the ACMA's consultation questions

Appendix 1 contains our answers to the twenty-four questions contained in the consultation paper.

1. Do the proposed amendments to the ECS Determination fulfil the objectives and content requirements of the direction? If not, please explain why, and describe any alternative or additional approaches that could be used to meet the objectives and requirements of the direction.

We consider that the proposed amendments to the ECS Determination generally fulfil the objectives of the Minister's direction.

Our submission does propose five minor changes to the draft Amendment Determination that will provide clarity to CSPs and MNOs, and allow MNOs to meet the obligations of the Amendment by 28 October 2024. See section 2 for details of the five minor changes we are recommending.

2. Is the ordinary meaning of mobile phone sufficient noting that the direction does not intend to inadvertently capture other communication devices such as internet of things devices or medical alert devices? If not, please explain what the definition of mobile phone should be and provide reasons.

We consider it is important to add the definition of a mobile phone. See section 2.5 for our views on this matter.

3. Can a carriage service provider currently identify whether the mobile phone that a customer proposes to use to access its network is configured to be able to access the emergency call service before service is supplied to that mobile phone?

No, an MNO or a CSP cannot identify whether the mobile phone a customer proposes to use is capable of making an emergency call, including camping-on to another mobile network, in advance of that mobile phone attempting to attach to the network. See section 2.2 for our views on this matter.

Our Recommendation 2 (see section 2.2) outlines a simple change to the drafting of the Amendment Determination, to resolve this matter.

4. Can providers currently identify whether a mobile phone that a customer proposes to use is configured to be able to access the emergency call service on the mobile networks **of other providers** before service is supplied to that mobile phone? [*emphasis added*]

No, not before the service is supplied (see section 2.2 and our answer to Q3 which explains it is not possible to identify a device before it attaches to the network), and also not without having first tested the device to understand its camp-on capabilities.

To fully understand whether a device will be capable of camping-on to another mobile network, it must be tested against Australia's actual mobile networks; it is insufficient to simply rely on vendor attestation against international standards (such as GSMA IR.92¹³). This is within the scope of the work contemplated by Recommendation 3 from the Bean Review.¹⁴ Also, Telstra tests the devices it sells through its retail channels for the ability to camp-on to other networks. Mobile phones should be tested for their camp-on capabilities either by the retailer who wants to sell the device, or through a Government

¹³ GSMA IR.92, ver 20.0. https://www.gsma.com/newsroom/gsma_resources/ir-92-ims-profile-for-voice-and-sms-20-0/

¹⁴ Final Report, DoITRDCA review into the Optus outage, 8 Nov 2023. <https://www.infrastructure.gov.au/departments/media/publications/review-optus-outage-8-november-2023-final-report>

funded testing facility on behalf of the whole industry. If a device is found to be unable to comply with emergency calling obligations, it should be recorded, and the TAC of the mobile phone added to an industry-wide TAC blacklist, which should be maintained and enforced by the Government or a Regulator, notionally the ACMA.

Once this blacklist is created, it would be possible for MNOs to deny access to those mobile phones, should they attempt to attach to a mobile network.

5. If the answer to either of Questions 3 and 4 is no, what additional information would be needed to give effect to such a requirement? Is that information currently available?

The answer to both Q3 and Q4 is no, but the reason is related to the use of the word “*before*” in the context of supplying a service. It is not possible to know what the mobile phone is *before* it attaches to the network.

When the mobile phone attempts to attach, further information is still required. As we noted in our answer to Q4, a blacklist of devices that have been tested and found to not be able to make an emergency call when authenticated onto the customer’s home network, or are unable to properly camp-on to another network to make an emergency call should be developed. Once the blacklist is developed, MNOs can implement a mechanism to deny those devices access to the mobile network, or to carriage services on their network.

6. If a mobile phone is configured to be able to access the emergency call service using both the network of the carriage service provider supplying carriage service to it, and the networks of other providers supplying carriage services to the public, can a carriage service provider that is supplying service to the mobile phone identify whether **that mobile phone will ‘camp-on’** to another network if required? If not, please explain why and indicate what additional information would be required to enable a carriage service provider to identify the ‘camp-on’ capability of a mobile phone. [*emphasis added*]

No, neither a CSP, nor an MNO can categorically know the camp-on capability of a mobile phone simply by observing its behaviour while attached to a mobile network. The only way to understand the camp-on capability is through independent testing of the device in a laboratory setting. See also, our answer to Q4.

7. What information do (or can) providers know about a mobile phone when it has connected to a provider’s network?

Providers can use the GSMA’s TAC database¹⁵ to find out more about the capabilities of a mobile phone, such as the mobile generations supported (3G, 4G, 5G), the 3GPP Bands supported, and other attributes such as VoLTE capability, or the need to rely on Circuit Switched Fall Back (CSFB).

However, we have identified errors in the GSMA’s TAC database, and while it is generally accurate, it cannot be fully relied upon in all instances. We recommend mobile network data (e.g., call records) are analysed to corroborate information in the GSMA’s TAC database.

¹⁵ GSMA Device Attribute database. See <https://www.gsma.com/solutions-and-impact/industry-services/device-services/gsma-device-attribute>

8. Can providers:
- (a) identify the make/model number of a mobile phone once it has connected to its network?
 - (b) share information with each other to identify mobile phones that cannot access the emergency call service on mobile networks?

8(a) – Yes. The TAC can be extracted from the IMEI once the device has connected to the network.

8(b) – Yes. MNOs can share information about the capabilities of devices, noting that any sharing of information is not automated through network interfaces, but is compiled “off-line” and shared manually.

9. Based on information that is available or will be available to providers on 1 November 2024, indicate the number or proportion of mobile phones to which providers currently supply service, that providers may no longer be able to supply service to because of the requirements in the draft amendments to the ECS Determination. Please explain your response indicating which provision/s is relevant to your answer.

[CIC Begins]

[CIC Ends]

10. What are the minimum reasonable steps that a carriage service provider should take to identify whether a customer’s mobile phone can access the emergency call service on their network and the networks of other carriage service providers?

All retailers of devices, including Carriers, CSPs and other device retailers including on-line suppliers have an obligation (under Australian Consumer Law) to ensure the devices they sell into the Australian market are fit-for-purpose, and comply with Australian standards and regulations. An industry-wide whitelist of devices that have been tested and are known to be able to make emergency calls directly on the customer’s home network, and through camp-on to another provider’s network, should be developed and maintained. This would allow any device retailer, and indeed, members of the public, the ability to obtain confirmation that the device they are selling (retailers) or buying (consumers) is able to access the emergency call service in all situations.

Once a register is established, the minimum reasonable steps any device retailer (Carrier, CSP or other device retailer) should take is to confirm that the devices they are selling are on the whitelist. This should be an enforceable obligation on all device retailers that is managed through the ACMA as part of its ongoing compliance work.

11. Should any groups of carriage service providers be exempt from the obligations? Or should there be different obligations on certain sub-sets of carriage service providers? If so, please explain.

[CIC Begins]

[CIC Ends]

12. Can a carriage service provider identify whether a mobile phone that it is supplying carriage services to can no longer access the emergency call service? If not, what, if any, additional information would providers need to identify such phones?

Q12 relates to s.64 of the Amendment Determination, which requires CSPs to identify whether the mobile phone the customer is using can “no longer access the emergency call service”. In the consultation paper, the ACMA makes it clear that this includes a user retrieving an “*older style mobile phone (for example as an interim measure because their usual mobile phone has stopped working)*”.¹⁶ The other obvious use case is where “something changes”, for example, an MNO closes an entire network generation (e.g., 3G) rendering any devices that relied solely on that network generation for emergency calls unable to make them, or the device itself changes, for example because of an over-the-air firmware upgrade.

In short, CSPs (MVNOs) will not have visibility of the types of events that would cause a customer to *no longer* be able to access the emergency call service, including network decommissioning, device firmware upgrades, or the customer changing-over to an older device. For more details, see our answers to previous questions and section 2.2 of our submission.

13. Does this raise any issues for end-users that should be considered?

Q13 relates to s.65 of the Amendment Determination, and the ACMA is asking whether the “... *notify end-users when their mobile phone is not able to access the emergency call service and to stop supply of carriage services within a specified period ...*”¹⁷ creates any issues.

Blocking the device (described in section 2.1) will deny the customer access to all carriage services, and section 0 of our submission describes what is possible in terms of notifications, before and after the mobile phone has been denied access to the network.

14. Is the rolling set of notifications to ensure that end-users have sufficient time to change mobile phones before their services are disabled appropriate? If not, why not?

Our observation is that regardless of the duration afforded to consumers to upgrade or change devices, people will often leave it to the last minute. We have been notifying customers that we’re closing our 3G network for five years, and yet there are customers still using 3G only phones. We know from our experience with closing the 2G network that these customers will only replace their devices once the network has been closed.

So, we recommend a short period of time, certainly no longer than four weeks, and note that many customers who are served notice under s.65 of the draft Amendment Determination, will wait until after their device has been denied access to the network before they take any action.

15. Should any other information be included in notifications to help the end-user to prepare for the disabling of their carriage services and prompt them to action?

No, there is no need for any other information to be included. Details of alternative devices, especially low-cost devices, and details of assistance for people experiencing financial hardship will suffice.

¹⁶ Consultation paper, bottom of p.3.

¹⁷ Consultation paper, p.4 in relation to Q13.

16. Noting that the disabling of service to an end-user's mobile phone will require the end-user to obtain another mobile phone, do providers have any data available or information relevant to the assessment of the likely cost of this requirement to end-users of mobile services?

The cost of a new mobile phone varies dramatically from below \$100 for refurbished phones, to thousands of dollars for current generation, top-end mobile phones.

17. Should the Determination specify the acceptable forms of notification, or leave this undefined to provide flexibility to carriage service providers to determine appropriate methods of notification?

We consider it is not appropriate to specify the acceptable forms of notification in the Determination. As we noted in section 0, once a mobile phone is denied access to the network, it is no longer possible to provide notification through that mobile phone (e.g., SMS or RVAs). This requires the CSP or MNO to revert to other notifications, such as email, post or information on a website. The CSPs and MNOs understand their target markets/demographics best, and can tailor notifications to those markets using the best available channels.

18. Should any groups of carriage service providers be exempt from the obligations? Or should there be different obligations on certain sub-sets of carriage service providers? If yes, please explain.

Q18 is in relation to s.66 of the proposed Amendment Determination, which requires CSPs to ensure their payment assistance policy includes at least one method by which customers in financial hardship can receive assistance to obtain a low-cost or no-cost mobile device that can access the emergency call service. Telstra has its payment assistance policy available on its website.¹⁸ Our customers can also call us to find out details.

Payment assistance plans are aimed at consumer and small business channels-to-market, and we consider there is no need to exempt a CSP who supplies a mobile phone service (not necessarily the device) to consumer or small business markets. If, however, a CSP only supplies enterprise markets where payment assistance is not required or available, we have no objection to those CSPs being exempted.

A CSP who only operates an on-line presence (not a bricks-and-mortar presence) should not be exempted purely because they have no physical presence.

19. Are carriage service providers able to confirm that a person requesting the supply of a mobile service is a foreign traveller to Australia and the period of time that such a person may intend to stay in Australia?

CSPs (MVNOs) are very unlikely to be able to identify foreign travellers; International roaming agreements are forged between network operators (MNOs), not the virtual operators (MVNOs). In addition, as we outlined in section 0, foreign travellers who purchase a (local) prepaid SIM in Australia are indistinguishable from an Australian resident purchasing a prepaid SIM, and it is not possible for CSPs or MNOs to identify foreign travellers in this context.

¹⁸ Telstra payment assistance policy, available at: <https://www.telstra.com.au/aboutus/support-in-times-of-need/adversity-financial-hardship>

20. Where a foreign traveller roams on more than one network in Australia, the proposed amendment would require all carriage service providers that handle roaming to comply with the notification requirement. Is this appropriate? If not, why not?

We note that the clause relating to foreign travellers (s.67) is an exception from complying with s.63 and s.65. An exception is not a mandatory requirement (obligation), it is simply the opportunity to not have to comply with the obligations to which the exception applies. In this regard, we do not agree with the ACMA's interpretation as phrased in this question, "**roams on more than one network**", firstly because roaming may not be the only method by which a foreign traveller is identified (the Amendment Determination does not mention "roam" or "roaming"), and secondly, where roaming is the mechanism used to identify that the customer is a foreign traveller, the traveller need only roam on to one network, not more than one.

We also do not agree with the premise of the question, that the amended ECSD will *require* CSPs (technically, MNOs) that handle roaming to **comply** with the notification requirement of s.67(b), because s.67 itself is an exception and there is no obligation to take advantage of the exception afforded by s.67.

However, should an MNO wish to avail itself of the exception in s.67, then we agree clause 67(b) does *require* the MNO to send a notification to the foreign traveller before the mobile phone they are using can be excepted from being denied access to the network. We consider that sending a notification is an appropriate thing to do, and we support the language and obligation proposed by clause 67(b).

A final point of note in relation to this question, is that as outlined in section 4 of our submission, our proposed blocking implementation will not be able to identify and isolate international roamers or foreign travellers more generally (see section 0) .

21. Should the exception involving foreign travellers in Australia be limited to situations where the carriage service provider is being approached in Australia to supply services? This would exclude the requirements from applying to international roamers. If not, why not?

We do not see the need to limit the exception afforded by s.67 to only apply where the traveller approaches an Australian CSP to supply a service. In principle, if some travellers to Australia are to be granted an exception, then all travellers to Australia should receive the benefit of that exception, regardless of whether or not they present themselves to an Australian CSP.

For completeness, we note again that we will not be able to identify foreign travellers under our proposed blocking implementation. See section 0 and section 4.

22. Is the 60-day period for foreign travellers to use carriage services on mobile phones that are not able to access the emergency call service appropriate? If not, why not, and what alternative timeframe would be appropriate?

The 60-day period is reasonable.

23. For carriers and carriage service providers, what are the likely costs and benefits of implementation for your organisation? (Please provide specific cost estimates in your response.) Are there alternative ways to achieve the objective of the direction that would be consistent with its terms and provide for lesser costs and/or greater benefits?

The benefit of introducing the amendments to the ECSD, is that it will give MNOs and MVNOs the legislative framework required to deny customers who persist in retaining mobile phones that will not be able to access the emergency call service, from accessing a mobile network with those devices. This in turn gives customers certainty about being able to make an emergency call after the closure of the remaining 3G networks.

The cost to consumers arises from forced replacement of a device that might have otherwise suited their needs. If the customer is using a 4G-Data/3G-Voice device¹⁹ purely for the purpose of accessing data (i.e., they have no intention of using “traditional” network-based voice calls), then when the amendments to the ECSD come into effect, the customer will have to replace that device, when it could have continued to serve their needs.

From Telstra’s perspective, there are costs in implementing the network mechanism to detect devices that are known to not be able to access the emergency call service (i.e., implement the “blacklist” lookup described in section 4). Also from Telstra’s perspective, and likely from the other CSPs’ and MVNO’s perspectives, there are also costs associated in training contact centre staff and retail outlet staff to deal with inquiries, and potentially cost in dealing with customer complaints, should the customer still be unsatisfied with our response(s) to their inquiry(s).

24. The ACMA is seeking feedback on whether there are:

- Additional matters aligned to the objectives that should be included in the proposed amendments to the ECS Determination?
- Matters included in the proposed amendments to the ECS Determination for which alternative arrangements that should be considered?

Please provide evidence to support your position.

We have outlined a few additional matters in the body of our submission, which we commend to the ACMA.

¹⁹ i.e., a device that is capable of using 4G data but requires a 3G network to make any network-based voice-call, including calls to the emergency call service. Note: voice calls through apps such as WhatsApp and Messenger only use data service, so a 4G-Data/3G-Voice device could make calls through these apps after the 3G networks are closed, but it is not possible to call the emergency call service through these apps.