Investigation Report

File No.	ACMA2023/633
Relevant entities	Optus Mobile Pty Limited ACN 054 365 696 Optus Networks Pty Limited ACN 008 570 330 Optus Internet Pty Limited ACN 083 164 532 Optus Fixed Infrastructure Pty Limited ACN 092 450 783 Collectively, **the relevant Optus entities** or **Optus**.
Relevant legislation	*Telecommunications (Emergency Call Service) Determination 2019* (**the Determination**) *Telecommunications Act 1997* (**the Act**) *Telecommunications (Consumer Protection and Service Standards) Act 1999* (**the TCPSS Act**)

Summary of findings

1. The Australian Communications and Media Authority (the **ACMA**) finds that by failing to comply with the Determination, as set out in **Attachment A**:

   a) Optus Mobile Pty Limited ACN 054 365 696 (**Optus Mobile**) contravened subsection 148(1) of the TCPSS Act on 4,560 occasions;

   b) Optus Networks Pty Limited ACN 008 570 330 (**Optus Networks**) contravened subsection 148(1) of the TCPSS Act on 113 occasions;

   c) Optus Internet Pty Limited ACN 083 164 532 (**Optus Internet**) contravened subsection 148(1) of the TCPSS Act on 24 occasions; and

   d) Optus Fixed Infrastructure Pty Limited ACN 092 450 783 (**Optus Fixed Infrastructure**) contravened subsection 148(1) of the TCPSS Act once.

2. The ACMA also finds that, as a consequence of contravening subsection 148(1) of the TCPSS Act as set out above:

   a) Optus Mobile contravened subsection 68(1) of the Act on 17 occasions;

   b) Optus Networks contravened subsection 68(1) of the Act on 21 occasions; and

   c) Optus Fixed Infrastructure contravened subsection 68(1) of the Act once,

   by failing to comply with the carrier licence conditions set out in Schedule 1 to the Act; and

   d) Optus Mobile contravened subsection 101(1) of the Act on 4,543 occasions;

   e) Optus Networks contravened subsection 101(1) of the Act on 92 occasions; and

   f) Optus Internet contravened subsection 101(1) of the Act on 24 occasions,

   by failing to comply with the service provider rules set out in Schedule 2 to the Act.

Background

3. The Determination imposes requirements on carriers, carriage service providers (**CSPs**) and the emergency call persons in relation to access, carriage, handling and transfer of calls to the emergency call service. Carriers and CSPs are required to comply with the Determination under subsection 148(1) of the TCPSS Act. Sections 68 and 101 of the Act also require carriers and CSPs to comply with carrier licence conditions and service provider rules. Carrier licence conditions and service provider rules include a requirement to comply with the Act, including the TCPSS Act.

4. The relevant Optus entities are each a carrier and/or a CSP, as set out below. Therefore, each entity must comply with the Determination.

Entity	*Role*	*Description of services*
Optus Mobile	Carrier and CSP	Mobile services and licensed carrier
Optus Networks	Carrier and CSP	Fixed-line and mobile services and licensed carrier
Optus Internet	CSP	Fixed-line and internet services
Optus Fixed Infrastructure	Carrier and CSP	Licensed carrier operating controlled networks and controlled facilities used to carry emergency calls.

5. On 8 November 2023, the Optus network experienced a nation-wide outage affecting Optus fixed phone, internet and mobile services (**the outage**). The outage also impacted CSP resellers of Optus' network. The outage commenced around 4am AEDT and continued for approximately 12 hours, with services being restored by 4pm AEDT the same day.

6. On 13 November 2023, the ACMA commenced an investigation under section 510 of the Act into the relevant Optus entities' compliance with the Determination, the Act, and the TCPSS Act in relation to the outage.

7. On 5 September 2024, the ACMA provided its preliminary findings to Optus ('**the preliminary findings**') and invited it to respond. Optus provided its response to the preliminary findings on 24 September 2024 ('**Optus' 24 September 2024 response**').

8. In reaching these findings, the ACMA has considered:
   > Information provided by Optus on 22 January 2024 (**1st response**) and 18 March 2024 (**2nd response**) in response to notices given by the ACMA under section 521 of the Act.

> Public submissions made to the inquiry into the Optus Network Outage conducted by the Senate Standing Committee on Environment and Communications (**the Senate inquiry**).[1]

> Information that Optus shared with the ACMA relevant to the review into the outage conducted by the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (**the Department's review**).

> Optus' 24 September 2024 response to the preliminary findings and clarifying information provided to the ACMA on 15 October 2024.

The outage

9. The outage occurred when [redacted] routers that form part of Optus' core network automatically self-isolated to protect themselves from an overload of internet traffic. This caused a loss of connectivity for fixed-line and mobile services, some enterprise services, and Optus' Operations and Maintenance (**the O&M**) network.[2]

10. The increase in routing information occurred after a routine software upgrade in one of Optus' international upstream transit networks, the Singtel internet exchange (**STiX**). STiX routers in North America were upgraded, causing traffic to be re-routed to one of the available alternate paths into the Optus network, a STiX peering router located in Asia. The re-routing of traffic occurred as expected for such an update and was in line with global peering arrangements.

11. As a result of the traffic re-routing, the Optus network received a large increase in routing information.[3] The routing changes propagated through multiple layers of Optus' network. When the changes reached the core network the increase in traffic exceeded pre-set safety limits on some of the routers. The self-protection limits on the routers were default settings that had been established by a third-party equipment vendor from whom the routers were sourced. Those settings could be, but had not been, changed.

Findings and reasons – Compliance with the Determination

Subsection 11(1)

12. Subsection 11(1) of the Determination requires carriers and CSPs to maintain, as far as practicable, the proper and effective functioning of their controlled networks and their controlled facilities that are used for the carriage of emergency calls to the emergency call service.

13. The ACMA has formed the view that Optus Mobile, Optus Networks and Optus Fixed Infrastructure failed to maintain the proper and effective functioning of their controlled networks and controlled facilities on 8 November 2023 for 2 reasons as set out below.

Network resiliency to protect the core routers

14. The self-isolation of the [redacted] core network routers caused the outage to the controlled networks and controlled facilities of Optus Mobile, Optus Networks and Optus Fixed Infrastructure and prevented the carriage of emergency calls over the Optus network.

---

1 https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/OptusNetworkOutage/Submissions

2 Used to monitor network elements, such as the status of base stations.

3 Specifically, Internet Protocol version 6 (**IPv6**) information. IPv6 uses larger internet protocol addresses than the previous IP version (128-bit versus 32-bit), which uses more of a router's memory.

The ACMA considers that maintaining the proper and effective functioning of the core network routers is crucial to the proper and effective functioning of the controlled networks and controlled facilities of Optus Mobile, Optus Networks and Optus Fixed Infrastructure.

15. The re-routed traffic caused by the software upgrade propagated through several layers of the Optus network and did not cause other routers in other network layers to self-isolate. It therefore appears that the increase in router traffic was not unreasonable and the Optus network should have coped with this change.

16. After the outage, Optus had made immediate changes to its systems to avoid similar outages in future. These changes included:

    > making changes to international gateway routers that connect to peering partners to ensure that routes do not propagate in the same way again

    > increasing the connectivity between the enterprise and business network, and the consumer network

    > improving the availability and increasing the protection of the *management network* so it is not impacted in the same way during a similar outage (the ACMA considers that this refers to the O&M network, which is discussed in more detail below)

    > implementing a network-wide change freeze to ensure that there are no other impacts on the network during the period of an upgrade to provide network stability.

17. Optus took the steps described above to improve the resilience of the network within 9 days of the outage. It therefore appears that these changes were reasonably achievable. The ACMA considers that Optus had the existing capability, knowledge and resourcing to uplift their network's resilience and could have reasonably implemented these measures at any time prior to the outage. Such maintenance could reasonably be expected to have supported network maturity and resiliency and avoided the core network routers self-isolating in response to the increase in routing traffic.

18. In Optus' 24 September 2024 response, Optus argued that:

    > Prior to the outage it had taken *such steps as were practicable to establish a resilient and properly maintained network by making investments that were on par with the investments and steps taken by industry peers*.

    > Its quick response after the outage does not imply that Optus had not taken reasonably practicable steps to maintain its network before the outage, contending that it could not have taken those steps in advance because it was unaware of the key causes of the outage.

    > It continually reviews router management with its equipment vendors and also sought independent, external expert advice. No experts identified a need to alter the safety limit settings prior to the outage, nor was the potential for each of the relevant routers to self-isolate outlined as a risk.

19. In response to the above points, the ACMA considers that:

    > The mere fact that Optus has previously made certain investments in its network does not mean that those investments were necessarily successful in enabling

Optus to maintain the proper and effective functioning of its network, as demonstrated by the outage.

> Optus had a responsibility to manage its own network infrastructure such that it could comply with the obligations in the Determination. Optus has not provided persuasive evidence that it had taken action to identify and effectively mitigate risks in its systems – risks that were realised and caused this outage.

Operation of the O&M network

20. The outage also caused a loss of connectivity to Optus' O&M network. The O&M network is essential for maintaining the proper and effective functioning of the Optus network because it monitors the status of the network and is used to manage different parts of the network, including Optus Mobile's base stations.

21. The loss of connectivity to the O&M network made it difficult for Optus to identify that its 3G units continued to radiate a signal and maintain voice transmission capabilities during the outage. The 3G signal prevented most mobile devices from camping-on[4] to other networks when making emergency calls, even though the calls were unable to be carried by the Optus network. This meant that end-users using a mobile service supplied by Optus were unable to access the emergency call service during the outage. In a submission to the Department's review, Optus stated that in a scenario where the O&M network is available, it can power-down ('wilt') the 3G base station sites to enable end-users making emergency calls to camp-on to other networks.

22. In its submission to the Senate inquiry, the Internet Association of Australia stated that:

    Industry best practice is to continuously monitor the performance of network elements through a separate 'out-of-band' network that operates completely independently to the network Optus uses to provide services to customers. This same out-of-band network should be used to gather logs for diagnostic purposes. In addition to a completely separate out-of-band network, this system should be further supplemented by a system to monitor the monitoring system from a network external to Optus altogether.[5]

23. The ACMA considers that at the time of the outage Optus had failed to take practicable steps to implement out-of-band (**OOB**) network connections to effectively manage the network in the event of an outage. The ACMA considers that Optus had insufficient OOB connections either to the O&M network, or direct connections to different parts of its controlled networks and controlled facilities. The Optus O&M network is critical and should have been designed and configured to reduce dependence on the core network such that the risk of cascading failures was reduced to an acceptable level.

24. In Optus' 24 September 2024 response Optus noted that the OOB network is not used to carry emergency calls to the emergency call person and is therefore not subject to section 11 of the Determination. Optus also advised that it was in the process of making enhancements to the OOB network at the time of the outage and

---

4 Camp-on is an arrangement that enables an end-user using a mobile telephone service to make emergency calls using a telecommunications network other than the end-user's home network. This may occur because the end-user is outside of their home network's coverage, or the home network is otherwise unable to carry the calls.

5 https://www.aph.gov.au/DocumentStore.ashx?id=92be4d79-f1fa-47b1-a8d2-024a2aa50431&subId=750371

had those enhancements been completed the OOB network would not have been impacted by the outage.

25. The ACMA rejects this contention. Optus' failure to implement appropriate OOB network connections is relevant because the failures relating to the O&M network meant that the broader Optus network did not function properly and effectively during the outage. The effective operation of the OOB network could have reduced the scope, impact and duration of the outage by providing Optus with a reliable method for performing maintenance on the affected parts of the Optus network. This is particularly relevant to the failure to wilt the 3G mobile towers (being part of Optus' mobile network), which prevented Optus end-users from camping-on to alternate networks. Optus' mobile network is used to carry emergency calls and is therefore subject to section 11 of the Determination.

26. The ACMA acknowledges that Optus had identified the need to enhance the resilience of the O&M network prior to the outage and that such enhancements necessarily take time. However, the fact that the O&M network went offline during the outage indicates that the design of the O&M network represented a significant divergence from best practice at the time of the outage. As previously stated, the ACMA considers that the O&M network ought to have been designed and configured such that a failure in any other part of the Optus network does not, or is highly unlikely to, adversely impact the availability of the O&M network.

Finding: The ACMA finds that Optus Mobile, Optus Networks and Optus Fixed Infrastructure contravened subsection 11(1) of the Determination once each on 8 November 2023 by failing to maintain the proper and effective functioning of their controlled networks and controlled facilities and by failing to take practicable steps to ensure that:

a) the network was sufficiently resilient to protect the core network routers and handle a reasonable increase in traffic volumes; and

b) there was appropriate OOB access to various parts of the Optus network infrastructure to enable Optus to monitor and manage its controlled networks and controlled facilities, including mobile base stations.

Subsections 12(2) and 19(2) – exceptions to compliance obligations

27. Paragraph 12(2)(a) of the Determination states that sections 13 to 18 of the Determination do not apply if a matter beyond the control of a CSP materially and adversely affects the CSP's technical ability to give an end-user access to the emergency call service. Subsection 19(2) of the Determination similarly states that subsection 19(1) of the Determination does not apply if a matter beyond the control of a CSP materially and adversely affects the CSP's technical ability to carry an emergency call to the relevant termination point for the call.

28. The exceptions set out in subsection 12(1) and paragraph 12(2)(b) of the Determination are not relevant to this matter.

29. In its 1st response, Optus submitted that the outage was caused by a matter beyond its control because the software update that resulted in an increase to routing information was beyond its control. Optus stated that it had been notified that the upgrade would take place, but it did not have visibility of the extent to which the upgrade would cause an increase in traffic.

30. The ACMA accepts that the software update caused an increase to routing information, the consequences of which meant that Optus was unable to carry emergency calls to the relevant termination point and give an end-user access to the emergency call service. However, the ACMA considers that the outage was caused by the self-isolation of [redacted] core network routers. As the maintenance of those routers and the architecture and configuration of its network was within Optus' control, to that extent, the outage was preventable.

31. While the default limits on the routers were set by a third party, the response of the Optus network to the increase in routing traffic resulting from the upstream change in the STiX network was within Optus' control. Optus controls the configuration of its network and is responsible for preventing cascading failures by determining the circumstances in which routing changes propagate. This includes load balancing and utilisation of redundant paths to maintain continuity of service. Optus is also responsible for the architecture of its O&M network and the level of dependence the O&M network has on the core network. As set out above, there were reasonable steps that Optus could have taken prior to the software upgrade to improve the resiliency of the network to protect the core routers from the increase of routing information.

32. In Optus' 24 September 2024 response, Optus reiterated its position that:

    > the increase in routing traffic was beyond its control

    > the safety limits on the routers and the way those routers would behave when the safety limits were exceeded were not identified by the equipment vendor nor any of the external experts that Optus engaged to undertake reviews of the routers.

33. As noted above, the ACMA considers that the increase in routing traffic was not unreasonable because the re-routed traffic propagated through several layers of the Optus network and did not cause other routers in other network layers to self-isolate. Optus also stated that the network should have coped with the change. The fact that the equipment vendor or Optus' external experts did not identify any issues in relation to the management of its infrastructure prior to the outage does not absolve Optus of accountability or transfer the risk associated with poor configuration and change management away from Optus. The network infrastructure is ultimately Optus-owned, and Optus ultimately holds exclusive accountability for the appropriate acquisition, configuration and ongoing management of it.

34. Therefore, the ACMA considers that the exceptions set out in paragraph 12(2)(a) and subsection 19(2) of the Determination do not apply because the outage was not caused by a matter beyond the control of Optus. Accordingly, the ACMA considers that sections 15, 17 and subsection 19(1) of the Determination apply to the relevant Optus entities.

Section 15

35. Section 15 of the Determination states:

    (1) If:

    (a) a CSP supplies an emergency telephone service; and

    (b) an end-user makes an emergency call on the service using the emergency service number 000,

the CSP must give the end-user access to the emergency call service operated by the emergency call person for 000 and 112.

*(2) If an end-user uses the emergency service number 112 on a public mobile telecommunications service (**PMTS**), the CSP who supplies the service must give the end-user access to the emergency call service operated by the emergency call person for 000 and 112.*

36. In Optus' 24 September 2024 response Optus disputed that section 15 of the Determination is relevant to this matter, arguing that the requirement is not to connect actual calls, but to ensure that the network is configured in such a way that it will enable calls to be connected to the emergency call service, if such calls are made.

37. The ACMA rejects this contention. Section 15 of the Determination imposes an obligation on a CSP to give *access* to an emergency call service to an end-user in the circumstances described. Section 18 of the Act states that a person is taken to not have access to an emergency call service unless, in the event that the person attempts to place a call to the relevant emergency service number, the call can be established and maintained. Section 15 of the Determination is therefore directed to establishing and maintaining the call under section 18 of the Act. Accordingly, the ACMA considers that section 15 of the Determination requires a CSP to provide access to the emergency call service for each end-user who uses the CSP's emergency telephone service or PMTS to make an emergency call by establishing and maintaining that end-users call, not just configure its network in the way suggested by Optus. If Optus fails to establish and maintain the call in those circumstances, it will not have given the end-user access and will contravene section 15 of the Determination.

38. In Optus' 24 September 2024 response Optus also provided details about 28 test calls made by Optus employees. The ACMA accepts that these calls were not emergency calls and therefore they have been removed from the findings.

39. Therefore, the ACMA finds that on 8 November 2023:

    a) Optus Mobile contravened section 15 of the Determination on 2,091 occasions;

    b) Optus Networks contravened section 15 of the Determination on 41 occasions; and

    c) Optus Internet contravened section 15 of the Determination on 12 occasions,

    for the reasons set out below:

Element	Evidence and assessment
The relevant Optus entity is a CSP that supplies an emergency telephone service	In its 2nd response (and clarified in response to the preliminary findings): > Optus Mobile provided a list of 2,091 calls made by end-users to whom Optus Mobile supplies an emergency telephone service. > Optus Networks provided a list of 42 calls made by end-users to whom Optus Networks supplies an emergency telephone service.

	> Optus Internet provided a list of 12 calls made by end-users to whom Optus Internet supplies an emergency telephone service. The total 2,145 calls are set out at **Attachment B.**
An end-user makes an emergency call on an Optus service using the emergency service number 000 OR An end-user makes an emergency call on an Optus service using the emergency service number 112 on a PMTS	2,144 of the 2,145 calls listed in Attachment B were made by end-users to either 000 or 112 (one call was made to 106 by an end-user on a service supplied by Optus Networks).
Optus must give the end-user access to the emergency call service operated by the emergency call person for 000 and 112	Optus Mobile, Optus Networks and Optus Internet failed to give the relevant end-users access to the emergency call service because the 2,144 calls were unable to be established and maintained, and therefore were not answered by the emergency call person.

Finding: The ACMA finds that on 8 November 2023:

a) Optus Mobile failed to give 2,091 end-users who made emergency calls to 000 and 112 using an emergency telephone service supplied by Optus Mobile access to the emergency call service operated by the emergency call person for 000 and 112;

b) Optus Networks failed to give 41 end-users who made emergency calls to 000 and 112 using an emergency telephone service supplied by Optus Networks access to the emergency call service operated by the emergency call person for 000 and 112; and

c) Optus Internet failed to give 12 end-users who made emergency calls to 000 and 112 using an emergency telephone service supplied by Optus Internet access to the emergency call service operated by the emergency call person for 000 and 112,

as required by section 15 of the Determination.

Section 17

40. Section 17 of the Determination states that if an end-user uses the emergency service number 106 on a carriage service that is a standard telephone service as described in subparagraph 6(1)(b)(ii) of the TCPSS Act, the CSP must give the end-user access to the emergency call service operated by the emergency call person for 106.

41. Subparagraph 6(1)(b)(ii) of the TCPSS Act sets out that a standard telephone service includes a carriage service for the purpose of a form of communication that is equivalent to voice telephony for a particular end-user with a disability (for example, a teletypewriter).

42. Optus disputed that section 17 of the Determination is relevant to this matter for the same reasons set out in relation to section 15 of the Determination above. The ACMA disagrees for the same reasons. The ACMA considers that if an end-user uses the emergency service number 106 on a carriage service that is a standard telephone service, Optus must give that end-user access to the emergency call service by establishing and maintaining the end-user's call. A failure to do so constitutes a contravention of section 17 of the Determination.

43. Therefore, the ACMA finds that Optus Networks contravened section 17 of the Determination on one occasion on 8 November 2023, for the reasons set out below:

Element	Evidence and assessment
An end-user uses the emergency service number 106 on a carriage service described in subparagraph 6(1)(b)(ii) of the TCPSS Act.	One call listed in Attachment B was made to 106 by an end-user on a fixed line service supplied by Optus Networks.
Optus Networks must give the end-user access to the emergency call service operated by the emergency call person for 106.	Optus Networks failed to give the relevant end-user access to the emergency call service because the call was unable to be established and was therefore not carried to the relevant termination point for the call, to be answered by the emergency call person for 106.
Finding: The ACMA finds that on 8 November 2023, Optus Networks failed to give one end-user who used the emergency service number 106 access to the emergency call service operated by the emergency call person for 106, as required by section 17 of the Determination.	

Subsection 19(1)

44. Subsection 19(1) of the Determination requires a CSP that supplies an emergency telephone service to ensure that an emergency call made using the service is carried to the relevant termination point for the call:

    a) on the CSP's telecommunications network, or

    b) if the CSP's telecommunications network does not allow direct delivery to the relevant termination point for the call – by another telecommunications network.

45. In Optus' 24 September 2024 response Optus provided details about 28 test calls made by Optus employees. The ACMA accepts that these calls were not emergency calls and therefore they have been removed from the findings.

46. The ACMA finds that on 8 November 2023:

    a) Optus Mobile contravened subsection 19(1) of the Determination on 2,091 occasions;

    b) Optus Networks contravened subsection 19(1) of the Determination on 42 occasions; and

c) Optus Internet contravened subsection 19(1) of the Determination on 12 occasions,

for the reasons set out below:

Element	Evidence and assessment
The relevant Optus entity is a CSP that supplies an emergency telephone service	Attachment B sets out: > 2,091 calls made by end-users to whom Optus Mobile supplies an emergency telephone service > 42 calls made by end-users to whom Optus Networks supplies an emergency telephone service > 12 calls made by end-users to whom Optus Internet supplies an emergency telephone service.
An emergency call made using the service	The total 2,145 calls listed in Attachment B were made by those end-users to 000, 112 or 106.
Optus must ensure that the call is carried to the relevant termination point.	In its 2nd response, Optus Mobile, Optus Networks and Optus Internet stated that the 2,145 calls were not carried to the relevant termination point for the call. Section 6 of the Determination defines the relevant termination point as the point in the network of the emergency call person reasonably specified by that person as the point to which a call must be carried.
Finding: The ACMA finds that on 8 November 2023: a) Optus Mobile failed to carry 2,091 emergency calls made using emergency telephone services supplied by Optus Mobile to the relevant termination point for the call; b) Optus Networks failed to carry 42 emergency calls made using emergency telephone services supplied by Optus Networks to the relevant termination point for the call; and c) Optus Internet failed to carry 12 calls made using emergency telephone service supplied by Optus Internet to the relevant termination point for the call, as required by subsection 19(1) of the Determination.	

Paragraph 27(2)(b)

47. Section 27 of the Determination applies if a significant network outage adversely affects a controlled network or controlled facility that a carrier or CSP:

    a) owns or operates; and

    b) uses to carry emergency calls or supply emergency telephone services.

48. Paragraph 27(2)(b) of the Determination requires the carrier or CSP, as soon as possible after becoming aware of the outage, to notify, or arrange to notify, each CSP

in relation to whom the carrier or CSP has an obligation to provide access under section 10 of the Determination of the outage.

49. The ACMA finds that on 8 November 2023:

    a) Optus Mobile contravened paragraph 27(2)(b) of the Determination on 16 occasions; and

    b) Optus Networks contravened paragraph 27(2)(b) of the Determination on 20 occasions,

    for the reasons set out below:

Element	Evidence and assessment
A significant network outage that adversely affected a controlled network or controlled facility that Optus owns or operates and uses to carry emergency calls or supply emergency telephone services.	In the 1st response, Optus Mobile, Optus Networks and Optus Fixed Infrastructure confirmed that at the time of the outage they were using controlled networks and controlled facilities to carry emergency calls to the emergency call service. The outage adversely affected these controlled networks and controlled facilities. Section 6 of the Determination defines a significant network outage as an unscheduled network failure that adversely affects the carriage of emergency calls over that network in a significant way, having regard to: > the number of customers impacted by the outage > the likely amount of time it will take to restore carriage services disrupted by the outage > the availability of other carriage services that can be used by affected customers to make and receive calls. The ACMA considers that the outage of 8 November 2023 was a significant network outage of the Optus network. The outage was lengthy and nation-wide, causing Optus end-users to lose service (apart from one exchange that maintained connectivity). Accordingly, section 27 of the Determination applies to Optus Mobile, Optus Networks and Optus Fixed Infrastructure and the ACMA has considered whether Optus Mobile, Optus Networks and Optus Fixed Infrastructure complied with their obligations under paragraph 27(2)(b) of the Determination in the row below.
Optus must notify, or arrange to notify, each CSP in relation to whom Optus has an obligation to provide access under section 10 of the Determination as soon	In its 2nd response, Optus Mobile provided a list of 16 CSPs and Optus Networks provided a list of 20 CSPs that they provided with access to controlled carriage services, controlled networks and controlled facilities under section 10 of the Determination. These CSPs are listed in **Attachment C**.

as possible after becoming aware of the outage.	Optus Fixed Infrastructure stated that it does not provide any such access to CSPs. In its 1st response, Optus explained that it primarily relied on national media channels to notify CSPs that utilised the Optus network, including social media (Facebook and X), media releases and updates published to its website. These appear to be statements addressed to a broad public audience rather than to the CSPs themselves. The ACMA considers that relying solely on such general public communications through national media channels rather than notifying or arranging to notify each of the CSPs does not meet the notification requirements under paragraph 27(2)(b) of the Determination. In Optus' 24 September 2024 response Optus acknowledged that it contravened paragraph 27(2)(b) by failing to directly notify the CSPs identified in the preliminary findings of the outage.
Finding: The ACMA finds that: (a) Optus Mobile failed to notify, or arrange to notify, 16 CSPs; and (b) Optus Networks failed to notify, or arrange to notify, 20 CSPs, in relation to whom they have an obligation to provide access under section 10 of a significant network outage affecting their controlled networks and controlled facilities, in accordance with paragraph 27(2)(b) of the Determination.	

Subsection 28(1)

50. Subsection 28(1) of the Determination requires a CSP, as soon as practicable after becoming aware of a significant network outage that adversely affects a controlled network or controlled facility that the CSP owns or operates, to undertake, or arrange to be undertaken, a welfare check on an end-user who made an unsuccessful emergency call during the outage using an emergency telephone service supplied by the CSP.

51. Subsection 28(2) of the Determination states that subsection 28(1) does not apply where:

    a) the CSP cannot identify that the end-user has made the unsuccessful emergency call;

    b) the CSP is satisfied that the end-user subsequently made a successful emergency call; or

    c) the end-user made the unsuccessful emergency call using a PMTS, and the location of the customer equipment from which the call was made has changed since the call was made.

52. In Optus' 24 September response Optus provided details about 28 test calls made by Optus employees. The ACMA accepts that these calls were not emergency calls and therefore they have been removed from the findings.

53. The ACMA finds that:

    a) Optus Mobile contravened subsection 28(1) of the Determination on 361 occasions; and

    b) Optus Networks contravened subsection 28(1) of the Determination on 8 occasions,

    for the reasons set out below:

Element	Evidence and assessment
End-user made an unsuccessful emergency call during a significant network outage using an emergency telephone service supplied by Optus.	The ACMA considers that the outage of 8 November 2023 was a significant network outage of the Optus network as defined by section 6 of the Determination. Attachment B lists a total of 2,145 unsuccessful emergency calls made during the outage, of which: > 2,091 were made by end-users using an emergency telephone service supplied by Optus Mobile > 42 were made by end-users using an emergency telephone service supplied by Optus Networks > 12 were made by end-users using an emergency telephone service supplied by Optus Internet.
Optus must as soon as practicable after becoming aware of the outage, undertake, or arrange to be undertaken, a welfare check on the end-user who made the unsuccessful emergency call during the outage.	Based on the 2nd response and Optus' 24 September 2024 response, the ACMA accepts that: > Optus conducted welfare checks as soon as practicable after becoming aware of the outage for 183 of the 2,145 calls > the exception in paragraph 28(2)(b) of the Determination applies for 31 of the 2,145 calls because the end-user subsequently made a successful emergency call that camped-on to the Telstra network > the exception in paragraph 28(2(c) of the Determination applies for 1,562 of the 2,145 calls because the location of the PMTS from which the call was made changed since the call was made.[6] This leaves a total of 369 calls for which welfare checks were required to be undertaken. Section 6 of the Determination defines a welfare check as the process of checking on the safety and well-being

[6] Some of the end-users who had moved location also subsequently made calls that camped-on to Telstra. Ultimately, the exceptions in paragraphs 28(2)(b) and (c) of the Determination combined apply to a total of 1,593 calls.

	of an end-user that made an unsuccessful emergency call. The Determination sets out minimum steps the CSP must follow to contact the end-user by phone or by SMS. If the CSP is unsuccessful in contacting the end-user, the CSP should refer the matter to a State or Territory police force. In Optus' 24 September 2024 response, Optus acknowledged that it contravened subsection 28(1) of the Determination by failing to undertake a welfare check. This statement relates to the 369 calls mentioned above, being 361 Optus Mobile end-users and 8 Optus Networks end-users who made unsuccessful emergency calls on 8 November 2023.

Finding: The ACMA finds that:

a) Optus Mobile failed to undertake, or arrange to be undertaken, welfare checks on 361 end-users who made an unsuccessful emergency call during the outage using an emergency telephone service supplied by Optus Mobile; and

b) Optus Networks failed to undertake, or arrange to be undertaken, welfare checks on 8 end-users who made an unsuccessful emergency call during the outage using an emergency telephone service supplied by Optus Networks,

as required by subsection 28(1) of the Determination.

Findings and reasons – Compliance with the carrier licence conditions and service provider rules.

Subsection 148(1) of the TCPSS Act

54. As carriers and/or CSPs, the relevant Optus entities must comply with the relevant requirements imposed by the Determination under subsection 148(1) of the TCPSS Act.

Finding: The ACMA finds that due to the outage of 8 November 2023:

a) Optus Mobile contravened subsection 148(1) of the TCPSS Act on 4,560 occasions;

b) Optus Networks contravened subsection 148(1) of the TCPSS Act on 113 occasions;

c) Optus Internet contravened subsection 148(1) of the TCPSS Act on 24 occasions; and

d) Optus Fixed Infrastructure contravened subsection 148(1) of the TCPSS Act once,

because they did not comply with the requirements of the Determination, as set out above and in Attachment A.

Subsections 68(1) and 101(1) of the Act

55. Subsection 68(1) of the Act provides that a carrier must not contravene a condition of the carrier licence held by the carrier. The standard carrier licence conditions are set

out in Schedule 1 to the Act and include, at clause 1 of Part 1 of Schedule 1, a requirement that the carrier must comply with the Act and the TCPSS Act.

Finding: The ACMA finds that in their capacity as carriers:

a) Optus Mobile has contravened subsection 68(1) of the Act on 17 occasions;

b) Optus Networks has contravened subsection 68(1) of the Act on 21 occasions; and

c) Optus Fixed Infrastructure has contravened subsection 68(1) of the Act once,

because they did not comply with the requirements set out in sections 11 and 27 of the Determination and therefore have not complied with the TCPSS Act.[7]

56. Subsection 101(1) of the Act provides that a CSP must comply with the service provider rules. The rules are set out in section 98 and Schedule 2 to the Act. Schedule 2 to the Act includes, at clause 1 of Part 1 of Schedule 2, a requirement to comply with the Act and the TCPSS Act.

Finding: The ACMA finds that in their capacity as CSPs:

a) Optus Mobile has contravened subsection 101(1) of the Act on 4,543 occasions;

b) Optus Networks has contravened subsection 101(1) of the Act on 92 occasions; and

c) Optus Internet has contravened subsection 101(1) of the Act on 24 occasions,

because they did not comply with the requirements set out in sections 15, 17, 19 and 28 of the Determination and therefore have not complied with the TCPSS Act.[8]

ATTACHMENTS

A: Summary of findings –contraventions of the Determination

B: Contraventions of sections 15 and 17 and subsections 19(1) and 28(1) of the Determination

C: List of CSPs relevant to paragraph 27(2)(b) of the Determination.

[7] As set out in Attachment A, these figures relate to the following potential breaches:
- Optus Mobile: 1 for ss11(1) and 16 for para 27(2)(b)
- Optus Networks: 1 for ss11(1) and 20 for para 27(2)(b)
- Optus Fixed Infrastructure: 1 for ss11(1).

[8] As set out in Attachment A, these figures relate to the following potential breaches:
- Optus Mobile: 2,091 for s15, 2,091 for s19 and 361 for ss28(1)
- Optus Networks: 41 for s15, 1 for s17, 42 for s19 and 8 for ss28(1)
- Optus Internet: 12 for s15 and 12 for s19