



Submission to the Australian
Media and Communications
Authority

**Review of the Numbering
Plan: Reply to
Submissions**

Public Version

August 2024

OVERVIEW

1. Optus welcomes the opportunity to provide additional comments to the Australian Media and Communications Authority (ACMA) responding observations made in the first round of submissions to the review of the Numbering Plan.
2. Optus observes that the Australian Government has a very clear policy position on the need to protect Australians from scams. The Assistant Treasury The Hon. Stephen Jones MP outlined this policy in his address to the National Press Club on '*Fighting Scammers, Fighting for Australians*' on Wednesday, 31 July 2024. Notably, he observed that Australians no longer trust phone numbers, meaning "Consumers aren't answering calls from call centres because it might be from a scammer."
3. Optus shares these concerns. We also see that Australians are no longer trusting phone numbers – no longer trusting that Australian numbers come from Australia; no longer trusting that mobile phones calls are coming from mobile phones.
4. The Australian Government expects industry to do more. The Assistant Treasurer called for "Telcos and social media need to cut off the means of communication and publication." Optus agrees with these sentiments. It is clear that there is the means and opportunity for CSPs to do more, and that they must. The first step is to return trust to the Australian numbering system.
5. There are some CSPs who wish to continue some current practices, and to continue to flaunt the existing legislation and regulations that form the construct of how numbers can be used. In other words, they wish to continue the practices that have led to Australian no longer trusting numbers and no longer answering phone calls. This would appear counter to Australian Government policy and counter to the intent of the Numbering Plan.
6. Some of those CSPs say that we should continue to rely on tracebacks to stop scams. In other words, to shut the barn door after the horse has bolted. Evidence shows this is not working. Continuing with the status quo is not a viable option.
7. A significant further reduction in scam calls and scam SMs is within reach for the telco industry, although there are parts of the industry who still oppose this. This must be opposed. The existing rules – when enforced – are enough to bring trust back to Australian numbers.
8. The industry can only do this if the ACMA steps up and ensures that the Australian numbering system can again be trusted by the public.

ERODING TRUST IN MOBILE NUMBER RANGES

9. In this section we respond to claims made by some CSPs who are seeking to widen the use of mobile numbers beyond mobile networks. Worrying, some CSPs appear to admit that they are using numbers in a manner inconsistent with the Numbering Plan. We welcome the ACMA's view on whether such behaviour warrants further investigation.
10. We note that Commpete, In their submission states that:

allocating specific number ranges for specific technologies has merits where there is a need to route traffic in a particular way, or where there are merits in customers and/or networks being able to recognise that a specific number type is associated with traffic or a specific and predictable type. However, allocation for the most trusted number ranges, such as 04 numbers, should not be limited to established carriers or prohibited for innovative users.
11. We observe that '04' numbers are trusted because there is a reasonable assumption that the use of these numbers would be in accordance with the existing regulatory construct on the use of numbers, and that there would be an individual with a mobile phone on the other side of the call. Mobile numbers have this high level of trust because MNOs have not generally permitted mobile numbers held by non-MNOs to be provisioned on their networks.
12. However, we observe that mobile number continue to be allocated by the ACMA to non-MNOs, and appear to be increasingly used by non-MNOs. As a result, the trust in this number range has been eroded by the misuse of this number ranges, either by scammers or through call centres and debt collectors using these numbers through VoIP services.
13. Such use is in breach of the Numbering Plan, which states that a Digital Mobile Number must be used with Public Mobile Telecommunications Service (PMTS), which is defined in s.32 of the Telecommunications Act and requires that the service to be supplied by use of a Telecommunications Network that has Intercell Hand-over functions such as PLMNs (Public Land Mobile Networks).
14. Extending the use of mobile numbers beyond use by MNOs will undermine the very trust in the '04' range that creates the demand to access these numbers by non-MNOs.
15. We also observe that some CSPs appear to misunderstand the current rules. For example, Voxbone "opposes proposals aimed at allocating digital mobile numbers exclusively to MNOs. Such a move would stifle competition, hinder development, and disrupt the existing market ecosystem where numerous innovative services are currently provided by non-MNOs using these numbers." Similarly Pivotel state that mobile numbers should be used for services "other than a mobile handset directly connected to a mobile network and the numbering plan should accommodate these in order to maintain an efficient and competitive marketplace"
16. Such statements misunderstand the current regulatory arrangements, for which this restriction is already in place. Any allocation that has been applied for and received by a non-PMTS operator is not permitted under the Numbering Plan. Telecommunications is a competitive environment, and a CSP can today work with an MNO to use Digital Mobile Numbers through their PMTS as their MVNO. Optus would be concerned if Voxbone or Pivotel are using mobile numbers in a manner inconsistent with the Numbering Plan.

17. We also note that Symbio makes similar comments that the “Rules that apply to this number type should recognise that the use of mobile numbers has changed over recent times, including the manner by which services have been delivered to mobile numbers, e.g. via Wi-Fi, via cloud based services and potentially via LEO satellite services.”
18. Optus observes that the methods suggested by Symbio are not necessarily against the existing rules where calls are still provided through PMTS networks. For example, WiFi Calling, will still route the call back through the Home PLMN, and future use of LEO constellations will also route calls back through its Home PLMN. The issue is where non-PMTS networks attempt to use mobile numbers for what are essential fixed networks.
19. The position of some CSPs appear to be that existing rules that are aimed at protecting the integrity of mobile numbers should be changed to permit current non-compliant uses of these numbers. Optus does not agree with this concept. Rather, where CSPs state that they are using numbers in a manner inconsistent with the Numbering Plan, the ACMA should investigate further – and where warranted commence compliance action.

MULTIPLE SERVICES TO A NUMBER

20. **Commpute** commented on the use of a number for outbound calls from a different CSP than issued the number to the customer:

Commpute views the provision of numbers, (and the associated inbound termination service) and the provision of outbound termination services as distinct services provided to and purchased by customers of CSPs.

In our view, numbers are purchased and can be used by businesses and consumers primarily as a standalone product, enabling a reply-path to the communications they are sending, but also often for branding purposes on outbound communications, so that consumers can become accustomed to interacting with them via a consistent set of phone numbers.

21. In our initial submission, Optus identified a range of instruments that would require changes for the above concept to be legal in Australia. It is perhaps a lack of enforcement of the existing construct for many years that has led to this misunderstanding.
22. For example, *C555:2020 Integrated Public Network Database (IPND) Industry Code* requires that:

4.2.1 Each CSP that provides a Carriage Service to a Customer using a Number must provide the IPND Manager the relevant PNCD, including transaction updates, in respect of each Carriage Service it supplies, that occur on one Business Day, by the end of the next Business Day. This includes all transactions relating to connections or disconnections.
23. IPND does not support multiple CSPs listed against a number, so it is clear that any CSP that has been offering outbound calls as a standalone product is breaching IPND requirements, and compliance action could be taken by the ACMA.
24. There is evidence that the ACMA may have enforced this requirement on one occasion. On 15 February 2024, the ACMA issued a media release on “Five telcos breached for allowing SMS scams” <https://www.acma.gov.au/articles/2024-02/five-telcos-breached-allowing-sms-scams>.

25. The ACMA announced that the following CSPs were found to have breached the Reducing Scam Calls and Scam SMS Industry Code:
 - (a) Message4U Pty Ltd (trading under the brand name Sinch MessageMedia)
 - (b) SMS Broadcast Pty Ltd
 - (c) DirectSMS Pty Ltd
 - (d) Esendex Australia Pty Ltd
 - (e) MessageBird Pty Ltd
26. Each was also found to have breached IPND Code requirements, and were issued a direction to comply. Whilst 4 of the 5 were found to have issued numbers to end-users and supplies or supplied carriage services to them without updating the IPND. Interestingly, in the case of MessageBird Pty Ltd, ACMA instead found that:

“On 24 May 2023, MessageBird stated it did not provide the IPND Manager relevant PNCD by the end of the next business day after they occurred on 1,785 occasions for carriage services under investigation which MessageBird supplies or supplied.”
27. The implication of finding that MessageBird, an SMS Aggregator breached IPND requirements by not providing information to the IPND for carriage services it supplies or supplied, is to confirm that this practice is prohibited.

Unwelcome Communications

28. Under CA C525:2023 *Handling of Life Threatening and Unwelcome Communications Industry Code*, if one of the customers of this illegal product was to make a series of unwelcome communications using this product, the B-Party telco would send the required notification to the A-Party supplier. Under this product, it would be difficult to determine who the A-Party suppliers are, particularly if there are multiple A-Party suppliers.
29. A problem arises when the legitimate A-Party CSP which holds the number, can't verify that a specific number of unwelcome communications were originated.

5.2.5 If an A-Party Supplier verifies there has been a Specified Number of Unwelcome Communications after receiving an Unwelcome Communications action request from a B-Party Supplier, then the A-Party Supplier must:

 - (a) Send an acknowledgement receipt of the Unwelcome Communications action request to the B-Party Supplier within one Business Day of receiving the Unwelcome Communications action request;*
 - (b) issue an initial warning letter to the Customer of that A-Party CSI within two Business Days of receiving the Unwelcome Communications action request to alert the A-Party Customer that the Carriage Service has been used for Unwelcome Communications and that a criminal offence may have been committed and that the IMEI of the mobile device which was used for Unwelcome Communications may be blocked across all mobile Carriers in Australia; and*
 - (c) respond to the B-Party Supplier within two Business Days of the issue of the request and advise the action that has been taken and provide, where known, the IMEI of the mobile device if the A-Party CSI is associated with a PMTS.*
30. The concept, as put forward by Commpete, undermines the requirements of the *Handling of Life Threatening and Unwelcome Communications Industry Code*, and would prevent action being taken in accordance with the Code.
31. Commpete's argument, is that regulatory obligations should not apply to suppliers who offer this product in contravention of the many regulations that exist. It is also to create an unfair playing field, where they offer products where all the regulatory burdens and

costs are shifted to the CSP that holds the number, without that CSP earning revenue associated with that service, to cover its costs.

Annual Numbering Charges

32. To level the playing field in this scenario, the *Telecommunications (Numbering Charges) Act 1997* and the *Telecommunications (Annual Charge) Determination 2014* would require amendment, to ensure that the CSP offering standalone outbound calling, to also pay to provide services using a number.

Lawful Interception, Data Retention, EMERGENCY CALLS, & Welfare Checks

33. The *Telecommunications (Interception and Access) Act 1979* would also require changes to provisions relation to Interception Capability Plans, Lawful Interception, Data Retention, Assistance to Law Enforcement and National Security Agencies (as would telco systems and processes), as an agency would not know where to send a warrant if interception of calls were required. Any provider who is currently selling such a telecommunication service is essentially providing ghost phones that can evade lawful interception.
34. Such a provider would also be violating the Assistance to Law Enforcement and National Security Agency provisions of the *Telecommunications Act 1997*.
35. Optus is also concerned that if one of our customers were to make an emergency call to Triple Zero, and the call was routed through an unauthorised CSP, that enhanced mobile location information such as SMSA-based MoLI, Push MoLI, Pull MoLI & AML would not be provided to the ECP & ESOs in accordance with the requirements in the *Telecommunications (Emergency Call Service) Determination 2019* and *CA G557:2023 Location Information for Emergency Calls*. This would have adverse impacts on an ESO's ability to provide assistance to the emergency caller in a life-threatening time-critical situation.
36. If that unauthorised CSP was experiencing a significant network outage, we also find it highly unlikely that welfare checks in accordance with the requirements in the *Telecommunications (Emergency Call Service) Determination 2019* would take place.

Rights of Use

37. Commpete also state that "*numbers are purchased*" by business and consumers, with the implication that they can be used in any manner desired by the customer, which is not the case. Optus addresses that point later in this document.

Competition and Portability

38. The fact remains that Australians have a highly competitive telecommunications market available to them, and through the *C570:2009 Mobile Number Portability Industry Code* and the *C540:2013 Local Number Portability Industry Code*, a customer can take their number to a vast range of CSPs if they find a product that suits them better than what is provided by their current CSP.

Commpete stated the following reasons a customer may use multiple suppliers:

Included as part of these services is the ability for end-users to define the CLI or sender ID their communications will present to their respective recipients, subject to rules imposed by the Scam Code.

The ability for end-users to utilise multiple CSPs provides them with a number of benefits, including

but are not limited to:

- *Service redundancy*
- *Throughput/performance enhancement*
- *Greater commercial leverage through more competitive supply*
- *Utilisation of features, products and/or technology unique to specific CSPs*

39. The C661:2022 Reducing Scam Calls and Scam SMS Industry Code (Scam Code) states that:

4.2.1 Originating C/CSPs must prevent carriage of calls where the A-Party does not hold Rights of Use to the Number.

40. While some CSPs offering standalone outbound call services conduct a verification process to ensure that the customer holds Rights of Use (ROU) to a number, this reflects a slim minority of overstamped or spoofed CLI calls that enter Tier 1 networks. We particularly note the remarks of **Telstra** in their submission, that:

"We estimate that at least 80% of calls received by Telstra from domestic carriers, who don't hold the numbers, are scams".

41. Where some CSPs are also transit providers, they will take in these calls upstream of them from sources that are likely overseas, and outside the reach of Scam Code and Australian authorities. It is not feasible, nor acceptable for this state to continue.
42. On the matter of service redundancy, a customer is welcome to procure services from multiple service providers, and this is something that we see from many enterprise customers. The key though, is that the legitimate use of these services requires the use of numbers that were issued by the CSP on the service they provide.
43. If a CSP is unable to provide the throughput or performance required by a customer, they are able to choose from a provider who can meet their needs, or to split their services across multiple providers, again, using the numbers provided by the CSP that issued them, on that service.

Rights of Use

44. **Pivotel** is one of the submitters who overstated the principles of Rights of Use:

43. Do you support the use of numbers by multiple CSPs? Why or why not?

43.1. Yes. Pivotel unequivocally supports the use of numbers by multiple CSPs as this enables a competitive marketplace whereby alternative providers are able to compete with incumbents for the provision of value-added services.

43.2. Under the Comms Alliance Industry Code, C566:2023 Number Management – _Use of Numbers By Customers, the end user retains the Rights of Use (RoU), not the CSP who holds the number. As such the end user has the right to dynamically choose who will provide certain elements of their service requirements, irrespective of the CSP that holds the number, subject to compliance with relevant industry codes and regulations. This allows number holder to negotiate call rates with multiple outbound calling providers while also improving service resiliency through

the use of multiple CSPs.

45. While the account-holding customer is the Rights of Use (ROU) holder, such a right is not unfettered. For example, CA C566:2023 *Number Management – Use of Numbers by Customers Industry Code* states that:

General Rights of Use and Customer Information

A ROU Holder as the right to:

(ii) originate communication via a Listed Carriage Service on the Network provided by that CSP

4.3.4 CSPs must consider a Number as issued at the time that a CSP or its delegate and the Customer agree to the provision of a specific number for the Customer's use in association with a Listed Carriage Service, to be provided on the Network provided by that CSP.

46. It is clear that the ROU holder has a right to use a number only on the network that provided the customer that number.
47. The CSP that holds a number with an annual numbering charge, as levied by ACMA is licencing the right to commercialise services using that number.
48. **Pivotel** made the following views of carriers and ownership of numbers:

***44. Can you provide some evidence / data of the benefits or harms of this practice?
Please provide details and indicate if this information is provided in confidence.***

44.1. There is a current misconception amongst some incumbent carriers that they own the number and all associated rights of use and as a result have implemented blocking of calls (and threatened SMS) of any calls that utilise their allocated numbers.

49. Optus does not agree with Pivotel's assessment of a "*misconception*" by carriers. The CSP who holds a number has a right to commercialise services using that number, as well as having the burden of legislative and regulatory obligations and costs relating to that service, for which the revenue from that service is intended to cover. Removing the source of revenue relating to those obligations creates an anticompetitive unfair playing field.
50. The ROU Holder is always free to choose the service provider that best meets their needs, and can port their services at any time.
51. **Twilio** also had similar comments

11.4 While numbers are allocated to CSPs by the ACMA, they remain the property of the Commonwealth and do not 'belong' to the CSP. In addition, the reality is that customers also have rights of use and a key interest in the numbers that are issued to them. The number identifies an individual or business, allowing them to make or receive calls or SMS. Numbers often reflect customer brand identity and are therefore very valuable to that customer.

52. **Twilio** further stated:

11.11 The Scam Code explicitly defines CLI spoofing as “the unauthorised use of a number by an end-user”. As noted above, CSPs and carriers do not own the numbers they are allocated, these belong to the Commonwealth and end-users may be granted rights of use over those numbers. The consumer should therefore have the right to choose how that number is used, whether that entails another CSP providing a service using that number or the porting of that number. Unfortunately, some legacy operators consider numbers to be their property.

53. **Pivotel** continued their argument on the use of numbers:

44.5. It is common practice for customers to acquire outbound call and SMS termination services from multiple CSPs in a competitive marketplace. It is important to note that, in particular, predominantly business end-users are able to purchase these services on a competitive basis and they are not prevented from doing so under the so called rights of use argument put forward by some carriers. The end-user of the service should also be in a position to define the caller line identification (CLI) or sender ID that their communications will display to recipients, in accordance with the rules set by the SCAM Code.

54. **Pivotel** restated their claim of CSPs being of the view that they owned numbers:

44.3. Inbound and outbound termination services should be considered as two separate services offered to and purchased by end-user customers of CSPs. End-users typically acquire an inbound call service with allocated numbers from a CSP who sets a monthly rate for supplying the number hosting and in-coming call routing services, as well as other associated services.

44.4. CSPs, typically acquire the numbers from a carrier who has the numbers provisioned across the carrier networks. The market for these services is highly competitive among CSPs, and carriers, and has resulted in end user charges for numbers and calls which are reflective of the underlying cost of providing the service. The cost to the carriers and CSPs of ‘owning’ the numbers is simply an input cost to the supply of the numbers and incoming call service to end users. A separate competitive market for the carriage of the outbound call, including the caller CLI, has resulted in end user charges for calls which are reflective of the underlying cost of providing the service.

55. **Symbio** is also of the viewpoint that the ROU holder has unfettered use of numbers:

44. It should be emphasised that it is End Users, particularly business users, who are requesting this type of service. Such customers have the Rights of Use, ROU, granted under the Use of Numbers Code, and it is the end user who has rights of how numbers are used and not the carrier who acquires the number ranges for allocation to end users. CSP’s are providing services to meet their needs.

56. Optus refers Pivotel, Twilio, and Symbio to our above comments on the Rights of Use of Numbers.

57. Optus acknowledges Pivotel’s comment that the telecommunications market is highly competitive. Customers have a choice of many providers who can legitimately hold numbers and issue them to their customers for use on the network provided by that CSP.

POTENTIAL SOLUTIONS

58. ACMA raised the 3 broad options for the use of numbers across multiple service providers:

- (a) No change/Status quo
- (b) Introduce rules to manage the multiple-service practice
- (c) Prohibit the multiple-service practice.

59. Optus has reviewed the comments of CSPs on this topic.

60. **Pivotal** stated a preference to continue with the status quo (option 1):

45. Which of the 3 potential options do you consider to be most viable in the circumstances and why? Please provide details.

*45.1. **Pivotal considers Option 1, Status Quo, to be preferable** in combination with a mandatory CSP register, sender-id register and existing obligations on CSPs under the Scam Calls and Scam SMS Industry Code.*

45.4. Hence Option 1 supported by increased compliance and enforcement around end user rights to use numbers would appear to be the most rational approach whereby the market is allowed to be competitive and flourish without restrictive practices being forced on the industry by large national incumbents.

61. **Vocus** expressed a similar preference:

Vocus further considers that:

• option 1 of no change / status quo to the regulatory treatment of multiple-service practice is the least disruptive across CSPs' and end customers' current operations, although we see merit in the introduction of rules to better support industry codes managing the prevention of scam and fraudulent calls, and ...

62. **Voxbone** was also of a similar view.

Voxbone advocates for the continued support of the multi-service practice under clear regulatory frameworks that protect consumer interests while promoting innovation and competition in the telecommunications sector. **We endorse the 'no-change' option** provided ACMA ensures and clarifies as needed that this practice is fully permissible under the Scam Code, thereby preventing incumbents from implementing any form of blocking. However, should ACMA determine that additional measures are necessary, we would favor a light regulatory approach, preferably within the scope of the Scam Code, that accommodates this practice and all the possible impacted use cases.

63. **Symbio** also stated that this use was longstanding

43. *Symbio support allowing the use of numbers by multiple carriage service providers (CSPs) which is a longstanding practise in Australia. It aligns with modern technological advancements and offers several significant benefits.*

64. Option 1, or the “*Status quo*”, would be to continue to ignore the construct on the permitted use of numbers, and to not enforce existing requirements. It is not suitable for this state to continue.
65. As Optus stated in our initial submission, this (and option 2) would be to accept a large volume of Scam Calls and Scam SMSs to continue to reach telecommunication users in Australia. This has proven to be a very expensive approach, for which individuals bear the cost of scams.
66. Optus has previously identified numerous laws, regulations, and Industry Codes that would need to be amended, for this to be permitted; which would be in addition to extensive network and IT systems conditioning costs and added compliance burden.
67. As has been established in this document, this is not permitted under the current construct, including the below:
- (a) C555:2020 Integrated Public Network Database (IPND) Industry Code
 - (b) C661:2022 Reducing Scam Calls and Scam SMSs Industry Code
 - (c) C525:2023 Handling of Life Threatening and Unwelcome Communications Industry Code
 - (d) Telecommunications (Numbering Charges) Act 1997
 - (e) Telecommunications (Annual Charge) Determination 2014
 - (f) Telecommunications (Interception and Access) Act 1979
 - (g) Telecommunications (Emergency Call Service) Determination 2019
 - (h) Telecommunications Act 1997
 - (i) C566:2023 Number Management – Use of Numbers By Customers Industry Code
68. A lack of enforcement has led to a range of problems for consumers.
69. **Symbio** also referred to reasons for multiple service providers:

45. *This service provides additional reliability/redundancy for customers particularly in the light of recent network outages and the emphasis on telecommunications as an essential service.*

70. **Vocus** also provided commentary on this topic:

Vocus supports the use of numbers by multiple CSPs (the multiple-service practice) and opposes the prohibition of the practice as it would:

- *make associated products and services unavailable to carriers and CSPs to ensure its own network resiliency through call termination service (CTS) products, as well as to customers*

(including both customer CSPs and end-users) who have legitimate business needs for their use, and ...

71. **Voxbone** also had similar remarks, although acknowledged porting:

The multi-service practice provides end-users with increased choice, fosters competition, introduces new services, and enhances redundancy in telecommunications offerings. This practice is not new and has become essential in the evolving cloud communications market, enabling a range of cost-effective opportunities for business end-users. While Voxbone encourages customers to port-in their numbers to mitigate this issue in the Australian market, it is ultimately the prerogative of the customer to determine the benefits of utilizing numbers in this manner.

72. As previously stated, on the matter of service redundancy, a customer is welcome to procure services from multiple service providers, and this is something that we see from many enterprise customers. The key though, is that the legitimate use of these services requires the use of numbers that were issued by the CSP on the service they provide.

73. If a CSP is unable to provide the throughput or performance required by a customer, they are able to choose from a provider who can meet their needs, or to split their services across multiple providers, again, using the numbers provided by the CSP that issued them, on that service.

74. We acknowledge Voxbone's comment that a customer is able to port-in their number to the service provider of their choosing.

75. **Symbio** stated a supposed use case:

Use Case: Temporary Supplier Switching

In scenarios where a customer needs to switch suppliers quickly due to capacity constraints (e.g., a surge in call centre demand), the ability to use numbers across multiple providers ensures continuity. For instance, during a major system overhaul or PBX replacement, businesses can use temporary numbers while maintaining their original CLI for outgoing calls. This flexibility allows for smooth transitions and minimises disruption.

76. An organisation is free to use as CSPs as they would like, and through Mobile Number Portability and Local Number Portability, they are also free to take their numbers with them, although the key is that the legitimate use of these services requires the use of numbers that were issued by the CSP on the service they provide.

77. **Symbio** commented on whitelisting numbers:

46. New rules should be cost efficient to implement and focus on the CSP servicing the end user. Some additional comments on the rules provided for consideration.

- *An industry whitelisting/allow list is feasible provided it is centralised, standardised and real-time (API access).*

78. While there have been suggestions of whitelisting numbers so they can circumvent protections that have been, or will be implemented by carriers, it isn't possible to whitelist them only for the ROU Holder, but rather, the numbers are made available for use by anyone. This may result in targeting of those numbers, and contributing to an increasing lack of trust in Australian numbers.
79. **Symbio** expressed a view that not complying with legislative and regulatory obligations should result in fewer costs:

• The suggestion that CSP B must pay a fee to CSP A adds additional overlay of cost and complexity into the industry. The hosting CSP is already compensated for costs by the customer via the hosting charge.

80. Symbio proposes to provide CSP services, whilst avoiding all the legislative and regulatory requirements of providing services. If released of these burdens, an uneven playing field is created, where all these costs are shifted to the hosting CSP which is obligated to comply with all the requirements.
81. **Vocus** acknowledged the overwhelming benefits of prohibiting the multiple-service practice:

option 3 of prohibiting multiple-service practice would ensure better number confidence but create significant disruption and adverse impacts on carriers, CSPs and end-users in a way not previously experienced in the industry. Whilst such a prohibition will likely disrupt scam and fraudulent call traffic, it will also disrupt the significant remainder of PSTN traffic used for legitimate purposes.

82. Optus agrees that option 3 (prohibiting the multiple-service practice) would ensure better confidence in numbers and would likely disrupt scam and fraudulent call traffic, although we disagree that it would create a significant disruption and adverse impacts. Customers would still be free to port their numbers to Vocus or other CSPs, and avail themselves of the highly competitive telecommunications market in Australia.
83. **Vocus** argued for more of the same to reduce scam traffic:

Vocus does not consider that legitimate use of the multiple-service practice to be a problem.

In addition to the supporting arguments outlined by the ACMA for option 3, we note that lawful intercept is often cited as an issue with multi-homed services. However, we submit that this has never been a problem in practice as carriers have readily cooperated with relevant law enforcement agencies in determining where traffic is being originated.

We further submit that the stronger monitoring and enforcement of the Scam Code and traceback to remove CSPs which commonly generate scam and fraudulent call traffic should address stakeholders' concerns regarding the practice. Such steps would negate the need for a blanket prohibition on multiple-service practice.

84. On lawful interception, where another CSP is using Optus numbers without prior arrangement or permission; and particularly where calls were transited through another carrier, this call may not touch the Optus network at all, and lawful interception would be impossible.

85. To counter this, warrants would have to be sent to multiple operators, resulting in an increase in the number of warrants each operator would have to process. This would strain existing resources and would result in increased costs for the CSPs issued warrants and for the agencies issuing an increased number of warrants.
86. On the suggestion of stronger monitoring and enforcement of Scam Code and traceback to remove CSPs that generate scam; traceback is an after-the-fact approach, and while still necessary, should not be the first line of defence. To have the greatest impact on reducing the level of scam calls and the financial losses these can incur, we have to prevent them from reaching Australians in the first place.
87. Optus is unaware of any CSP which has been blacklisted from providing traffic into Australia as a result of traceback activities. There is already too much secrecy in tracebacks so that providers can keep their commercial arrangements with suppliers of scam traffic hidden. ACMA is required to be kept in the loop on each leg of the traceback, although we are unaware of any actions to prohibit transit providers who are repeat offenders from bringing traffic into Australia.
88. **Voxbone** suggests that the Scam Code review committee resolve the issue:

Voxbone appreciates the opportunity to strongly support the use of numbers by multiple CSPs. We believe, however, that this issue would be better addressed in the upcoming review of the Scam Code.

89. There is a fundamental disagreement within the telecommunications industry on this issue. The issue was essentially deferred in the 2022 version of Scam Code. Communications Alliance has previously written to ACMA on this issue (as have individual CSPs), although there have been no substantive responses on this issue. This issue is not capable of being resolved within that code review committee.

KEEPING SCAM TRAFFIC ROUTES SECRET

90. Some organisations, in their submissions on which potential solution should be adopted, put forward that they want to maintain secrecy over the origination points and transit paths of scam traffic.
91. **Pivotel** stated that identifying the sources of scams should be prioritised:

49. Is legitimate use of the multiple-service practice a problem? Please explain and provide specific details.

49.1 Clearly the issue of SCAM calling as described in the ACMAs well considered discussion paper is a problem. Practices which address SCAM calling and SMs at the source, or where a SCAM call/message can be clearly identified, should be prioritised and preferred in light of the potential alternative, which is a more constrained market that leaves consumers with more limited choice and competition in terms of solution providers and solutions available.

92. Optus agrees with Pivotel, that it is important that knowledge of the origination point and transit paths of Scam Calls and SMs should be prioritised so that action can be taken against repeat offenders. Regrettably, too much information on the sources of scam traffic is hidden behind a veil of secrecy, apparently justified by commercial concerns.

93. Optus looks forward to Pivotal's presumed support in amending the Scam Code to make this information available, and providers being held accountable.

94. **Commpete** sided with secrecy over transparency for whitelisting numbers:

One of the options proposed would involve that CSP B providing CSP A with full details of the numbers it uses. If this option is pursued, it should not require divulging commercial information with other industry players in order to provide a service if done bilaterally. A central ROU verification registry (preferably a technology solution rather than a manual bilateral process solution) would be a preferable approach. The carrier which holds the number will continue to provide chargeable primary services to the customer.

95. **Virtutel** also stated that information should be restricted:

33. Should the ACMA consider enhancing its registers in the Numbering System to improve visibility of all current CSPs and the numbers they hold? Why or why not?

Although in theory Virtutel supports this, as it could eventually lead to better adoption of industry porting and reporting requirements, this register would need to be limited to the conditioned carrier viewing their own assigned number ranges only for privacy and commercial reasons. With access to the downstream CSP information only available to the ACMA and/or law enforcement. Virtutel however believes this platform should be cross shared with the IPND, which already is the defacto system for this information.

96. **Symbio** also supported maintaining secrecy:

Option 2 puts forward rules to manage the Multiple Service Practice. This could be compelling if these are done at a low cost to implement and focus on obligations on the CSP servicing the end user only.

Some of the rule examples listed do raise concerns:

- *One necessitated a CSP disclose its commercial information to another to facilitate service. Granting a single industry player exclusive access and control to this data could unfairly enhance their competitive advantage, particularly if they already hold a substantial market position.*

97. It is increasingly difficult to identify the source of Scam Calls and Scam SMSs, as most second-tier providers are highly secretive about which provider upstream of them sent them the scam traffic. In response to many reports made under Scam Code, Optus is constantly informed only that "our upstream provider has taken action" or that "Our upstream provider has determined that the calls are not scams" (or similar).

98. Not only have we not been provided anything to counter that scam calls have been blocked, but we are kept in the dark about who exactly has determined that the calls are allegedly not scam calls, or how many upstream links away the claim is being made.

99. An unsubstantiated claim by an unidentified party has zero credibility.

100. Although ACMA are required to have full visibility of the chain, these Scam Calls and SMS continue to get access to Australians; and the true source of these scams, or at least the chain of providers who are allowing them access, is being kept secret.
101. This secrecy allows providers to continue to accept traffic from unscrupulous sources, and arguments for greater secrecy in anti-scam arrangements serve only to kneecap efforts to fight scams.

CALLS ORIGINATED OUTSIDE AUSTRALIA

102. **Symbio** commented on this issue:

Traffic Origination from outside Australia

24. Symbio does not support the introduction of rules around the use of Australian Numbers to originate calls from outside Australia.

There are a growing number of business requirements that at times means that Australian numbers could originate outside Australia. One such factor is the growth in Business Process Outsourcing due to changing customer preferences, the adoption of cloud-based solutions, Australia's proximity to Asia, and a strong service sector. As businesses continue to look for ways to improve efficiency and reduce costs, the demand for outsourcing services is expected to increase in the coming years.

We believe that introducing rules around the use of Australian numbers from locations outside Australia would impede innovation and be complex and costly to implement.

103. **Symbio** further commented:

25. In relation to scam, the handling of incoming international calls with Australian CLI is handled in the Scam Reduction Code and this should continue to be the case. As stated Symbio holds the Numbering Plan should be a principles based document.

Symbio has long supported the introduction of an Australian adaptation of STIR/SHAKEN. The Australian adaptation can benefit of overseas learnings and along with proper KYC (Know Your Customer) process ensure suitability as a part of the implementation. Australian industry participants can enforce trust arrangements between service providers. This co-operation will assist in removing bad actors; the Scam Reduction Code, STIR/SHAKEN and other arrangements as part of the development of a suite of tools Industry utilise to proactively prevent scam.

104. **Vocus** commented on this issue:

Instead of a prohibition, we submit that the ACMA should consider rules allowing carriers to stop and block specific numbers used for illegitimate purposes, as well as restrictions on the use of Australian numbers for Australian residents and businesses with Australian operations only.

105. There are valid uses of Australian businesses running overseas call centres, although the Numbering Plan, lists the public numbers available, and states:

16 Numbers for use—public

(1) For subsection 455(3) of the Act, the numbers that are for use in connection with the supply of carriage services **to the public in Australia** are the following

106. To simply issue Australian numbers for use through international switches may not be permitted, although a reasonable approach would be for any Australian CSP offering services to foreign call centres, to bring that traffic directly into their Australian network, following all the proper KYC checks that would be expected.
107. Optus also addresses the issue of KYC checks and the nature of the transit market in this document, noting that transit providers will take in scam calls from upstream, from sources that are likely overseas, and outside the reach of Scam Code and Australian authorities. It is not feasible, nor acceptable for this state to continue.

EMERGENCY SERVICES

108. Voxbone questioned the relevancy of emergency service requirements:

Account for the challenges that technological developments pose in the context of A2P services provided over digital mobile numbers, such as the need to provide emergency services for services used in connection with A2P voice services. With the increasing need for businesses to use software platforms to better connect with their customers, there has been a spike in demand for numbering resources that support both voice and messaging. However, **Voxbone questions the relevance of maintaining Emergency Service requirements** in connection with a service that is provided to an 'application' as opposed to an individual end-user. We believe that in reviewing which rules should apply to this number type, ACMA should consider this and similar issues but, we understand that such an update may require amending the Telecommunications Act 1997 and the Telecommunications (Consumer Protection and Service Standards) Act 1999.

109. If you are supplying a carriage service to a customer in Australia, that customer must be able to access emergency call services. If a supplier can't provide this, they must not supply services in Australia.