TELSTRA GROUP LIMITED

Review of the Numbering Plan and other instruments – Telstra's reply to submissions

Confidential version

7 August 2024

[redacted]

Table of Contents

01 Introduction

We welcome the opportunity to reply to submissions received by the Australian Communications and Media Authority (ACMA) in their review of the Numbering Plan and other instruments.

The ACMA received 17 submissions in response to its discussion paper on the review of the Numbering Plan and associated instruments. While there is some consensus across submissions on various topics, there is a clear divide on the topics of carriage service providers (CSPs) originating calls using a number held by another CSP, CSPs using mobile numbers to originate non-mobile network traffic, and the practice of using Australian numbers to generate traffic from abroad.

The Australian Competition and Consumer Commission (ACCC) addressed all three matters mentioned above in their submission. They noted that scams are enabled by these practices, as well as unregulated use of SIM box technology and insufficient fraud controls for Application-to-person (A2P) SMS communications on the part of some operators.[1]

This reply submission contains 8 observations; the first 5 (in section 02) are general in nature and relate to submissions where the above topics are referred to and vary from Telstra's position, and the remaining 3 (in section 03) relate to specific matters in individual submissions.

02 General observations across submissions

2.1. Ensuring consumer confidence in numbers

Reflecting on Twilio's view *"…that numbers belong to the Commonwealth and not individual operators, even those to whom the numbers were originally allocated. They are a scarce resource and should be used and regulated in a way that promotes their utility to Australian consumers and businesses and the economy more broadly. They should not be allowed to become a new bottleneck in the hands of incumbent operators."*.

In recent times we have seen a devaluation of the numbering resource. Customers no longer trust unknown geographic numbers to the point where scammers have recently changed tactics and started using digital mobile numbers. We are now seeing customers not trusting unknown digital mobile numbers. This is not just an Australian phenomenon. Ofcom has recently commenced consultation seeking views and evidence on the effectiveness, costs, risks and timescales of different technical solutions to tackle scam calls from abroad which spoof UK mobile numbers.[2]

Unfortunately, the case presented in the submission made by Keith Edwards is all too common. He states, "*A phone is a vital communication tool in this modern world. It enables us to quickly reach friends, family, work colleagues, suppliers, and customers. Although caller ID enables identification of calls from friends and family, other contacts are frequently less obvious. Until about a decade ago, I felt confident that an unknown caller on my phone was still someone I was likely happy to speak with. Now, it is most likely (I'd say 90%) that a call from an Australian number not in my address book is a scam caller.*"

This is a regular message we hear from our customers and is why we have invested significantly in trying to reduce scam calls and messages.

It's concerning that such an environment has been allowed to develop, primarily as a result of some CSPs allowing their customers (including scammers) to use numbers held by another CSP. Stopping this practice would stop many scam calls and help restore confidence in Australian numbers. Despite

[1] ACCC submission page 2.

[2] Call for input: Options to address mobile spoofing - Ofcom, 2024.

Telstra and some other CSPs repeatedly raising this issue with the ACMA, no specific action has been taken to stop the practice.

The value of Australian mobile numbers did not evolve over night; it has been built up over close to 30 years, through robust regulation and control over how the numbers can be used.

If the ACMA does not act soon, we face a future where Australian numbers have little value and the long-term interests of end-users (LTIE) of carriage services (and services provided by means of those carriage services) are significantly diminished.

This diminishment is not limited to the telecommunications industry; it also affects other sectors. Numbers are relied upon and used in various ways to promote trusted interactions between institutions, government, businesses, and individuals.

2.2. CSPs originating calls using a number held by another CSP

A number of submissions make the case that there is no longer a 1:1:1:1 relationship between a CSP, number, user and location/connected premises/device.[3] This view contends that an inbound termination service and an outbound calling service associated with the same number can be distinctly separate services and provided by different CSPs.[4] They claim that end users have 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.[5]

There is no reliable method for another CSP to authenticate a customer of another CSP

It is unclear how this use of the same number by multiple providers can be effectively managed. For instance, if a customer disconnects their number with the primary CSP (the CSP that issued the number), the number needs to be quarantined for six or twelve months before it can be re-issued to a new customer. After disconnection or re-issuing of a number, there is no mechanism to confirm the quarantine status or whether the customer requesting service has rights of use, unless notified by that customer, assuming it is the same customer of the primary CSP.

Some submissions have argued that with the introduction of authentication processes such as two-factor authentication, CSPs could confirm ROU of a number.[6] For example, Symbio suggests for mobile numbers, sending a unique verification code via SMS or voice call to the number in question, and asking the end user to provide the code back as confirmation they have access to the number. This approach simply confirms a requesting party has access to the number (at that time), for example an employee of a business, and not that the user is the ROU holder. Even if ROU is held, as noted above, having ROU today does not mean ROU will be retained in the future.

Unlike mobile number portability, which requires pre-port verification (PPV) involving the sending of a unique code to the mobile number being ported for confirmation by the gaining CSP, a fraudulent port can often be detected immediately even after a successful PPV. This is because the ROU holder loses access to their mobile service, prompting escalation with their CSP and initiation of a port reversal. However, where secondary CSPs originate calls using a number held by another CSP following the use of unique verification code via SMS, the ROU holder may never be aware that their number is being used to make outbound calls through another CSP.

[3] Commpete submission page 2.
[4] Commpete submission page 7 and Pivotel submission paragraph 44.3.
[5] Pivotel submission paragraph 43.2.
[6] Symbio submission page 9.

There is no reliable method for another CSP to authenticate a customer of another CSP; only the CSP which holds the number and has issued the number (which includes ported numbers) is in a position to verify their customer and ROU holder. No submissions have addressed how this can be managed.

There is no certainty the practice of CSPs originating calls using a number held by another CSP can currently be managed efficiently and correctly. This results in different customers (including scammers) using the same number across multiple different CSPs simultaneously.

It is also unclear how CSPs using numbers held by another CSP can comply with regulatory obligations such as number portability, updating the Integrated Public Number Database (IPND), and lawful interception requirements.

Lack of certainty regarding the use of numbers allows all issued numbers to be spoofed or used for CLI over-stamping

Most customers are unaware that their number can be spoofed, and most would not want their number to be spoofed. However, the current lack of certainty regarding the use of numbers allows all issued numbers to be spoofed or used for calling line identification (CLI) over-stamping. This has created requests for protection from spoofing, i.e. via a so-called 'Do Not Originate' register.

If the ACMA forms the view that it is acceptable to use a number for outbound calls from a CSP other than the one holding the number, it will be necessary to amend multiple regulatory instruments. This must include an approach to prevent spoofing. All numbers should be protected from spoofing unless a customer consciously chooses to use their number with multiple CSPs.

Finally, we are strongly of the view that the end user has ROU with the CSP holding their number and while that number is issued to them. This does not extend to ROU with another CSP unless the number is ported to that CSP (or otherwise authorised by the CSP currently holding the number) so it becomes the holder of the number.

2.3. CSPs using mobile numbers to originate non-mobile network traffic

Telstra notes the ACCC's submission[7], which refers to its recent decision not to modify the Mobile Terminating Access Service (MTAS) service description. The ACCC concluded that changes to the MTAS service description were not necessary following its recent combined declaration inquiry. The ACCC's submission also emphasises the need to clarify ways in which non-mobile operators are using, and are intending to use, mobile numbers as part of the Numbering Plan review.

Telstra agrees that more clarity is required regarding the use of mobile numbers on non-mobile networks. The use of mobile numbers to originate non-mobile network traffic is impeding CSPs, including Telstra, from blocking scam calls in accordance with the requirements under section 4.6 of the Industry Code C661:2022 Reducing Scam Calls and Scam SMs. [redacted]

CSPs are cautious about taking such action as there is a risk it would also disrupt non-scam traffic generated where some CSPs are allowing mobile numbers to originate non-mobile network traffic, impacting genuine customer calls.

The issue is further exacerbated as the observed behaviour of scammers is to increasingly use mobile numbers, usually spoofing existing numbers, as mobile numbers have become more trusted than

[7] ACCC submission page 4.

geographic numbers, i.e. a party receiving a call is more likely to answer a call received from a mobile number than a call received from a geographic number.

We are strongly of the view that mobile numbers must only be used for traffic that originates from a mobile carrier's network.

Note: The above position supersedes and corrects the position in our original 8 July 2024 submission where we proposed that the Numbering Plan should clearly state that mobile numbers can only be used for traffic originating from a mobile carrier's network or authorised by a mobile carrier to originate from other networks.

2.4. Using Australian numbers to generate traffic from abroad

We note several submissions advocating for the continued use of Australian numbers to generate international traffic. We want to reiterate our experience in dealing with scam calls and messages. [redacted]

We direct ACMA's attention to Ofcom's publication, "CLI Guidance - Guidance on the provision of Calling Line Identification facilities and other related services."[8] This publication (in paragraph 4.19A) provides clear guidelines on when calls from outside the UK (or Crown Dependencies) can present a UK CLI as a Network Number. The publication (in paragraph 4.16) also states, "For calls originated on networks outside the UK, the responsibility to check the validity of the CLI Data falls on the Communications Providers (CP) at the first point of ingress to the UK network."

Further guidance is provided on paragraph 4.16, stating that for calls originating on networks outside the UK, the responsibility to verify the validity of the CLI Data falls on the CP at the first point of ingress to the UK network. This check may be performed by an international gateway provider or a provider that receives a call into the UK via a direct route. When a call has entered the UK network through an international gateway provider, it is expected that the UK provider that first receives the call from the international gateway provider reassures themselves (for example, through appropriate contractual arrangements) that the international gateway provider has conducted the relevant checks.

Telstra submits that similar, enforceable requirements need to be introduced in Australia. The obligation should require that carriers/CSPs accepting calls with Australian CLI into Australia must be satisfied that the use case is genuine. Calls must be blocked unless the carrier/CSP that is the first point of entry to the Australian network has verified a genuine use case. This is necessary to address the issue of the high volume of scam calls originating from abroad using Australian numbers.

2.5. Reliance on Scam code and introduction of STIR/SHAKEN as a default to allow current practices to continue

A number of submissions supporting the practices in 2.2, 2.3 and 2.4 above point to enhancing C661:2022 Reducing Scam Calls and SMs Code[9] and/or introducing STIR/SHAKEN protocols[10] to combat scam calls and messaging. However, scam activity becomes significantly more difficult to detect under these practices. This appears to be a default and disingenuous argument to allow CSPs to continue practices that place Australian customers in harm's way, whilst not really addressing harm.

[8] CLI Guidance: Guidance on the provision of Calling Line Identification facilities and other related services (ofcom.org.uk)

[9] Twilio submission page 25, Vocus submission page 3, Pivotel submission page 11 and Symbio submission page 4.

[10] Symbio submission page 4, Twilio submission pages 25 and 26; Virtutel submission pages 5 and 11, Pivotel submission page 11.

There are diverse views within the industry regarding the enhancement of the C661:2022 Reducing Scam Calls and SMs Code. Although industry can work constructively where there are diverse views, in this case, Telstra is not confident that industry will be able to find common ground to achieve viable solutions that can address all of industry's views.

We also refer the ACMA to the Communications Alliance correspondence of 24 January 2023, which details that the majority of members do not support the introduction of STIR/SHAKEN protocols. As detailed in the Communications Alliance correspondence, these protocols have not been effective in reducing scam calls and messages in other jurisdictions and are likely to result in significant costs for both the industry and customers.

Simply maintaining current practices, while depending on improvements to the C661:2022 Reducing Scam Calls and SMs Code, and the implementation of STIR/SHAKEN, may not be sufficient to meet the industry's needs in effectively combating scam calls and messages.

03 Specific responses to matters in individual submissions

3.1. Symbio – obligation to condition allocated numbers

The Symbio submission advocates for rules that will automatically oblige carriers to condition numbers in their networks if a number is allocated to a CSP[11], which would also imply sub-allocation. Telstra does not agree with this forced or automatic number conditioning approach. Telstra does not condition mobile numbers for CSPs that are not operating mobile networks or do not have a hosting carrier operating mobile networks.

Number conditioning in interconnect carrier networks is working effectively and efficiently under the current rules and uses a framework with appropriate guardrails.

New numbers allocated by the ACMA to the other interconnect carrier, as updated in the ACMA Numbering allocation database and/or as notified by the other interconnect carrier that match an existing contracted call case, are conditioned in Telstra's network (and vice versa) in accordance with the terms of the interconnect agreement following receipt of notice.

New numbers allocated to the other interconnect carrier for a new call case that is not currently active and is not covered by an executed agreement must be referred to the Telstra Wholesale Account Manager, and if appropriate a commercial negotiation will commence (the other carrier would need to provide traffic forecast information; details of proposed use, etc).

A review of background information occurs, including whether the proposed use of the numbers allocated is valid.

Once terms are agreed and documentation signed, network conditioning will proceed using the agreed process.

If an invalid use is determined, Telstra will advise the other carrier and network conditioning will not proceed.

3.2. Telstra as the administrator of the IPND

Twilio's submission questions the 'ownership' of the IPND, suggesting that its administration should be transferred to the ACMA or another independent body, rather than being managed by Telstra. Twilio asserts that giving any industry player access to this data could provide a market participant, who

[11] Symbio submission page 5.

already has significant market power, with a distinct competitive advantage and access to sensitive business information.[12]

Telstra strongly refutes the claim that it gains a competitive advantage or accesses sensitive information through its management of the IPND system and performing the IPND Manager role. Telstra is required to perform the IPND Manager role as part of its carrier licence conditions and has been doing so for many years. This is imposed on Telstra and strict privacy requirements apply through the Telecommunications Act 1997. Twilio has never directly raised these concerns with the IPND Manager or Telstra at any point during our stewardship of the IPND.

The IPND system and database is an asset of the Australian Telecommunications Industry, where the operation of the IPND Manager function and database undergoes an independent financial audit annually. The IPND system and database are located outside the Telstra Group and are supported and maintained by an independent organisation contracted by Telstra. The IPND system and database, including its operation, are designed to be portable for easy transfer to another party if Telstra is relieved of its obligation to support and maintain the IPND.

Individuals performing the role of IPND Manager do not have access to Telstra's business IT systems, except those necessary to operate and manage the IPND. These individuals operate separately from Telstra's Retail business units that perform marketing, product development, and retail activities.

IPND data cannot be shared with individuals or groups within Telstra who do not serve an approved purpose to use and receive it, as outlined in the IPND Scheme 2017 and the IPND Code.

Individuals performing the role of IPND Manager have limited access to IPND data and can only access data for the purpose of performing the IPND Manager role. These individuals are restricted to perform specific activities and must inform the regulator if maintenance of IPND data is undertaken.

Individuals performing the role of IPND Manager must engage IPND stakeholders equitably, as per obligations listed in the IPND Code. This includes CSP registration, Data Provider registration, Data User registration, provisioning IPND system access, and considering technical/functional changes to the IPND.

The protection and integrity of IPND data is the highest priority for individuals performing the role of IPND Manager. This also applies to Telstra's Cyber Security and IPND Support teams when reviewing and assessing IPND Security ongoing or for pending functional or technical changes to the IPND application or database.

3.3. Local Number Portability

Pivotel's submission notes complexities of fixed number porting related to physical lines and telephone exchanges should not apply to virtual fixed numbers where end to end porting times should mirror those of mobile number ports, and that an efficient and timely process whereby porting numbers between all CSPs will facilitate increased uptake with cloud applications and improve the competitive marketplace for inbound and outbound calling.[13]

Telstra would advise caution to taking a simplistic approach to Local Number Portability (LNP). All numbers are virtual, even those related to physical lines and telephone exchanges. Although many over the top CSPs may be eager to generate revenue more quickly, it's important to consider the potential risks. In cases where complex arrangements exist for providing a carriage service and associated telephone numbers, there is a risk of customers having service disruption and their networks compromised, if LNP is not managed correctly. It's common for the losing CSP to be left with the task of

[12] Twilio submission page 24.
[13] Pivotel submission page 9.

restoring services following a service disruption caused by a poorly executed port request, while the gaining CSP bears little responsibility. This situation calls for careful consideration and a balanced approach to responsibility.