Investigation Report

File No.	ACMA2018/409-15
Carriage Service Provider	Primus Telecommunications Pty Limited ACN 071 191 396
Type of Service	Carriage Service Provider
Relevant Legislation/Code	*- Telecommunications Act 1997* *- Industry Code (C555:2017) Integrated Public Number Database (IPND)*
Date	13 December 2018

Findings

The Australian Communications and Media Authority (the **ACMA**) finds that, on multiple occasions, Primus Telecommunications Pty Limited ACN 071 191 396 (**Primus**):

> contravened subsection 101(1) of the *Telecommunications Act 1997* (the **Act**), which requires a carriage service provider (**CSP**) to comply with the service provider rules that apply to it, by failing to give Telstra Corporation Limited (**Telstra**, or the **IPND Manager**) the information it reasonably required to provide and maintain the Integrated Public Number Database (**IPND**), thereby contravening the service provider rule in clause 10 of Schedule 2 to the Act;

> Contravened the following clauses of the *Industry Code (C555:2017) Integrated Public Number Database (IPND)* (the **IPND Code**):

- 4.2.1 – because Primus, a CSP that provides carriage services to customers using a public number[1], failed to provide the relevant public number customer data[2] to the IPND Manager in respect of certain carriage services Primus supplies;

- 4.2.11 – because Primus failed to ensure that the public number customer data it provided to the IPND Manager was accurate, complete and up to date; and

- 4.2.25 – because Primus failed to supply to the IPND Manager all public number customer data updates that occurred on one business day, by the end of the next business day.

---

[1] In this report, *number* and *public number* mean a number under the *Telecommunications Numbering Plan 2015*.
[2] As defined in the IPND Code, where it is also referred to as 'PNCD'.

Background

1. This report presents findings of an investigation conducted by the ACMA under paragraphs 510(1)(a) and (c) of the Act into whether Primus contravened the Act and/or an industry code registered under Part 6 of the Act.

2. The investigation commenced on 16 July 2018. On 18 July 2018, the ACMA issued Primus a notice under section 521 of the Act requiring the production of documents and information (the **Notice**).

3. Primus responded to the Notice on 15 August 2018.

4. On 11 October 2018, the ACMA issued preliminary findings to Primus. It responded on 25 October 2018.

Relevant facts

5. Primus is a CSP within the meaning of the Act[3]. Primus supplies telecommunications services (largely fixed-line) to residential and business consumers. It also provides services to other retail CSPs on a wholesale basis.

6. Primus is a 'Data Provider' within the meaning of clause 2.2 of the IPND Code.[4]

The IPND and its legislative framework

7. The IPND is intended to be an industry-wide database of all public telephone numbers. It was established in 1998 and is managed by Telstra as required by section 10 of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* (**Telstra Licence Conditions**). The maintenance of the IPND by the IPND Manager is supported by, among other things:

    a. a service provider rule requiring a CSP that supplies a carriage service to an end user, and where that user has a public number, to give Telstra such information as Telstra reasonably requires in connection with Telstra's fulfilment of its obligation to provide and maintain the IPND[5]; and

    b. the IPND Code, which is an industry code registered by the ACMA under Part 6 of the Act, and which sets out procedures relating to the storage of information in the IPND and the transfer of information to and from the IPND Manager.

8. The IPND Code, and the associated IPND Data Guideline (G619:2017), also refer to the *Integrated Public Number Database (IPND) Data Users and Data Providers Technical Requirements for IPND* (the **Technical Requirements**). The Technical Requirements, which are issued by Telstra and made with the agreement of a majority of relevant Data Users[6] and Data Providers (see clause 7.1.8 of the IPND Code), set out the detailed operational and technical requirements for the submission of information by Data Providers to the IPND Manager.

---

[3] See section 87 of the Act.
[4] 'Data Provider' is defined to mean a CSP who has an obligation to provide PNCD to the IPND Manager, or an entity acting on behalf of the CSP, and who is registered with the IPND Manager.
[5] Subsection 101(1) of the Act requires CSPs to comply with the service provider rules, and paragraph 98(1)(a) of the Act provides that the service provider rules include the rules set out in Schedule 2 to the Act. Clause 10 of Schedule 2 to the Act deals with the information that CSPs must give to Telstra in association with its IPND Manager responsibilities.
[6] As defined in clause 2.2 of the IPND Code.

9. The information in an IPND record includes customer name and address, phone number, the type of service, whether the service is listed or unlisted and details about the service provider. The Technical Requirements (at clause 6.1.2) specify the information that is included, or which can be included, in an IPND entry. An IPND record includes a mandatory field, called the 'Service Status Code', which is used to indicate whether a service is connected or disconnected.

10. Under Part 13 of the Act and the Telstra Licence Conditions, the information in the IPND can only be used for specific purposes. Critical users of the IPND include the emergency call service, the emergency warning system, and national security and law enforcement agencies. These bodies use IPND information to protect life and property and to investigate serious crime. Failure to provide accurate, timely and current information to critical users can have serious consequences. For example, failure to provide location information associated with a call to the Triple Zero emergency call service could place the caller's life at risk. Non-critical users of IPND data include publishers of public number directories and researchers conducting permitted research.

11. There are several ways in which a Data Provider can identify potential errors occurring when uploading data to the IPND, and any discrepancies between its own customer data and that stored in the IPND, including:

    > by reference to clause 4.2.28 of the IPND Code, which allows a Data Provider to obtain an extract of its public number customer data as a full set of records or a subset of records based on criteria agreed between the Data Provider and the IPND Manager for reconciliation purposes.

    > by reference to clauses 6.1.6 and 6.1.7 of the IPND Code, which require a Data Provider to download the information the IPND Manager produces about hard and soft errors[7], and take reasonable steps to resolve the matter and supply the corrected public number customer data to the IPND Manager within one business day for hard errors and two business days for soft errors.

    > additionally, the IPND Manager sends reminders via email (at least twice a year) to the approved contact(s) of all Data Providers about the importance of checking the corresponding error file after each IPND upload to ensure the file has been processed successfully.

    > by reference to clause 6.1.10 of the IPND Code, which encourages Data Providers to check a monthly 'changed data provider' report produced by the IPND Manager, which informs the Data Provider of all numbers gained and lost in the last month.

Primus' response to the Notice

12. Primus compared its customer database against its records in the IPND on 6 August 2018 (in responding to the Notice) which revealed that:

---

[7] 'Hard' and 'soft' errors are identified during the IPND's validation process when a Data Provider attempts to upload a file of IPND records (a file may contain one or more records). A hard error, such as mandatory field in the IPND record being blank, prevents the upload of the file and/or the record containing the hard error to the IPND.
A soft error is a possible error in an individual field of the record. In this case, the file is still uploaded to the IPND but is tagged as having a 'soft' error. A soft error can signify potential name and/or address inaccuracies, or missing information within an IPND record. The IPND Manager makes reports about hard and soft errors available to Data Providers.

a. 339,994 public numbers associated with a Primus 'active' service do not have a corresponding record in the IPND (missing records);

b. 5,010 public numbers associated with a Primus service have an incorrect Service Status Code in the corresponding IPND record (inaccurate records), comprised of;

   i. 2,295 public numbers associated with a Primus 'active' service which have a 'disconnected' status in the corresponding IPND record;

   ii. 454 records associated with Primus with a 'connected' status in the IPND are shown as 'disconnected' in Primus' customer database;

   iii. 2,261 records associated with Primus with a 'connected' status in the IPND are not present in Primus' customer database.

13. Primus also stated that:

a. the 339,994 records missing from the IPND were thought to be caused by Primus' customer systems not distinguishing between 'active' and 'connected' services for its ISDN 100 number ranges[8];

b. the inaccurate Service Status Codes were likely to be a result of timing issues with data uploads and file error corrections;

c. it would correct the IPND records with an incorrect Service Status Code by 17 August 2018. It had commenced work on creating the entries for numbers with no IPND record; and

d. it would:

   i. form a project task group with executive staff oversight to develop a solution in relation to the ISDN 100 number range issues;

   ii. create IPND process and training documents to be rolled out to relevant staff; and

   iii. for 12 months starting on 15 September 2018, conduct an audit of Primus' systems against the IPND every three months. Based on the results, it would then reassess the frequency of audits.

Primus' response to the Preliminary Findings

14. The ACMA's preliminary findings set out that Primus had contravened the service provider rule and the IPND Code in relation to:

a. **340,299** active services with no record in the IPND. This figure comprised the 339,994 numbers reported by Primus in response to the Notice, plus 305 numbers confirmed by Primus as missing records prior to the commencement of the investigation;

b. **5,011** IPND records for Primus services with an incorrect Service Status Code. This figure comprised the 5,010 numbers reported by Primus in response to the Notice,

---

[8] Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. A 100 Number ISDN Range is a series of 100 numbers that are allocated to ISDN business phone lines.

plus one number confirmed by Primus as having an incorrect Service Status Code prior to the commencement of the investigation.

15. In response to the Preliminary Findings, Primus submitted that it:

    a. continues to increase awareness of IPND processes among relevant managers, is documenting and formalising processes and training, and will conduct regular audits of its data against IPND data;

    b. accepts the findings and the reasons in the report regarding compliance with the Act and the Code with the exception of the number of instances of alleged contraventions in the preliminary findings report;

    c. believes that the number of public numbers associated with an 'active' Primus service with no corresponding record in the IPND should be reduced from the 339,994 advised in its response to the Notice to **11,817** because the original figure included numbers which:

        i. appeared in Primus' billing system but which were in use by other Vocus Group Limited entities (Primus is a subsidiary of Vocus) and for which an IPND record existed; or

        ii. were associated with wholesale services (that is, Vocus has sub-allocated the public number on a wholesale basis to another CSP which then provides the carriage service to the end-user and therefore is responsible for uploading IPND data); or

        iii. were used for 'inhouse' purposes including test services, inbound numbers (13, 1300, 1345 and 1800) used by Primus call centres, and 5,000 reserved numbers.

16. Based on information provided by Primus, the ACMA accepts Primus' submissions in relation to the services at subparagraphs 15c(i-iii) above, and has excluded them from further consideration.

17. Primus also indicated that it suspects that the remaining 11,817 missing records include a large number of 100 number ISDN range numbers and that not all numbers in these 100 number ranges are active. However, Primus had no evidence to support this at the time of its submission. Accordingly, the ACMA has included these in the contravention totals (11,817 plus 305 already admitted breaches is **12,122**).

Findings and reasons

Compliance with the Act

18. Subsection 101(1) of the Act requires that service providers, including CSPs, comply with the service provider rules that apply to them. Subsection 98(1) of the Act provides that the service provider rules include those set out in Schedule 2 to the Act.

19. Clause 1 of Schedule 2 to the Act provides that service providers must comply with the Act. Clause 10 of Schedule 2 requires that where a CSP supplies a carriage service to an end-user, and the end-user has a public number, the CSP must give Telstra (as the IPND Manager) such information as Telstra reasonably requires to fulfil its obligation to provide and maintain an IPND.

Clause 10 of Schedule 2

20. In determining what information the IPND Manager reasonably requires to fulfil its obligation to provide and maintain an IPND, the ACMA has regard to the Act, the Telstra Licence Conditions, the IPND Code and the Technical Requirements.

21. Subclause 10(4) of the Telstra Licence Conditions requires that the IPND must include, among other things, the public number, and the name and address of the customer. It is reasonable for the IPND Manager to require that information which the Telstra Licence Conditions require it to obtain, and which are obviously essential to the maintenance of the IPND.

22. Further, the IPND Manager may reasonably require other information that will assist in delivering the objectives of the IPND. Having regard to the critical functions described in paragraph 10 above, the ACMA considers that the service status of a number (that is, 'connected' or 'disconnected') is important to the proper functioning of the IPND, given that an incorrect status could adversely impact Data Users' services (noting that researchers and public number directory publishers only receive 'connected' records). It could also cause severe detriment in some cases (if, for example, a service did not receive an emergency warning because it was listed as 'disconnected').

23. The IPND Manager has explicitly sought the service status information from Data Providers in respect of each IPND entry, via the Technical Requirements. As noted above, the Service Status Code is a mandatory IPND field (others are optional), and the Technical Requirements have been made in consultation with, and with the agreement of, Data Providers. Further, clause 4.2.10 of the IPND Code provides that Data Providers must ensure that all public number customer data transferred to the IPND Manager is in the format specified in the Technical Requirements; and clause 4.2.11 provides that the Data Provider must ensure that the information provided to the IPND Manager is accurate, complete, and up to date.

24. Considering the above, the ACMA is satisfied that the IPND Manager reasonably requires CSPs to provide correct information about whether a telephone number is connected or disconnected to fulfil its obligations as IPND Manager. By uploading information that incorrectly identified connected telephone numbers as 'disconnected', and disconnected telephone numbers as 'connected', Primus did not give the IPND Manager the information it reasonably required to fulfil its obligation to maintain the IPND.

25. Based on information provided by Primus, it did not upload public number customer data to the IPND for 12,122 public numbers, and Primus customer data for 5,011 other public numbers had an incorrect connection status[9].

26. Primus has advised that the errors have occurred due to a range of technical and/or systems issues. This does not excuse or detract from Primus' responsibility to ensure that it gives the IPND Manager the information it reasonably required to fulfil its obligation to maintain the IPND.

27. The ACMA therefore finds that Primus contravened clause 10 of Schedule 2 to the Act.

---

[9] This investigation has not considered whether other fields in the relevant IPND records contain inaccuracies.

28. Accordingly, the ACMA finds that Primus contravened subsection 101(1) of the Act as it failed to comply with the service provider rule in clause 10 of Schedule 2 to the Act.

Compliance with the IPND Code

29. The IPND Code is an industry code registered under Part 6 of the Act[10] which applies to CSPs (among others).[11]

Clause 4.2.1

30. Section 4.2 of the IPND Code sets out rules in relation to the provision of data to the IPND Manager. As noted above, clause 4.2.1 of the IPND Code obliges a CSP to supply relevant public number customer data (also referred to as PNCD) to the IPND Manager for each public number it uses to supply a carriage service. Primus is a CSP within the meaning of the IPND Code.

31. Public number customer data includes, among other things, the public number, and the name and address of the customer, as referenced in the Telstra Licence Conditions and the definition in clause 2.2 of the IPND Code.

32. Based on information provided by Primus, it did not upload public number customer data to the IPND for 12,122 public numbers used in connection with an active, or previously active, Primus service.

33. The ACMA therefore finds that Primus contravened clause 4.2.1 of the IPND Code.

Clause 4.2.11

34. Clause 4.2.11 of the IPND Code requires a CSP to ensure that the public number customer data provided to the IPND Manager is accurate, complete and up to date.

35. Based on information provided by Primus, it did not upload public number customer data to the IPND for 12,122 public numbers, and 5,011 other public numbers had an incorrect Service Status Code.

36. The ACMA therefore finds that Primus contravened clause 4.2.11 of the IPND Code as it failed to ensure that the information it provided to the IPND Manager in those instances was accurate, complete and up to date.

Clause 4.2.25

37. Clause 4.2.25 of the IPND Code requires a CSP to supply to the IPND Manager all public number customer data updates that occur on one business day, by the end of the next business day.

38. Public number customer data updates can include a change to the customer data for an existing number, or any new or ported numbers for which customer data has not previously been provided by the CSP.

39. Based on information provided by Primus, no public number customer data for 12,122 public numbers was uploaded to the IPND by Primus and there was incorrect information in the IPND for a further 5,011 public numbers. Primus made no claim that these numbers were for services that were newly connected, ported or disconnected and that

---

[10] The IPND Code is registered under section 117 of the Act.
[11] See cl. 1.3.1(b) of the IPND Code.

the time limit for uploading or updating IPND customer data had not expired. Consequently, updates for these services were not supplied to the IPND within the requisite timeframe.

40. The ACMA therefore finds that Primus contravened clause 4.2.25 of the IPND Code by failing to supply public number customer data updates that occur on one business day, by the end of the next business day.