Investigation Report

Summary	
Entity	SMS Broadcast Pty. Ltd. (**SMS Broadcast**)
ACN / ABN	ACN 127 334 785
Type of entity	Carriage service provider (**CSP**)
Relevant Legislation	*Telecommunications Act 1997* (**Act**) Industry Code C555:2020 Integrated Public Number Database (IPND) (**IPND Code**) Industry Code C661:2022 Reducing Scam Calls and Scam SMs (**Scams Code**)
Date	15 November 2023

Findings

The Australian Communications and Media Authority (**ACMA**) finds SMS Broadcast has, as set out at Table 1 below, contravened the Act, IPND Code and Scams Code.

Table 1: Summary of contraventions

Legislation	Provision	Number of contraventions	Relevant period
Act	Subsection 101(1)	2,561	25 October 2019 to 8 June 2023
IPND Code	Clause 4.2.1	2,547	20 March 2020 to 8 June 2023
Scams Code	Clause 5.2.1	16,289	10 August 2022
	Clause 5.2.2	Estimated 4,588,941	12 July 2022 to 8 June 2023

Reasons

1. The ACMA's findings are informed by information and documents obtained from:

   a. SMS Broadcast on 24 May 2023 in response to a compulsory notice given by the ACMA under section 521 of the Act

   b. SMS Broadcast on 21 July 2023 in response to a request for additional information by the ACMA

   c. Telstra Ltd in its capacity as the manager of the Integrated Public Number Database (IPND) (the **IPND Manager**) on 1 and 5 April 2023

   d. SMS Broadcast on 29 September 2023, in response to the ACMA's preliminary findings

   e. traceback emails made by carriers and carriage service providers (**C/CSPs**) across the investigated period under the Scams Code, to which the ACMA is copied in.

Issue #1: IPND compliance

Background to the IPND

2. The IPND is a centralised database of public numbers[1] established in 1998. It is managed by the IPND Manager in accordance with section 10 of the *Telecommunications (Carrier Licence Conditions - Telstra Corporation Limited) Declaration 2019* (**Telstra Licence Conditions**), and under predecessor instruments before 2019.
3. CSPs must ensure that customer data about carriage services they supply to end users in connection with a public number is provided to the IPND Manager for inclusion in the IPND. Customer data is provided by Data Providers. A CSP can either act as its own Data Provider or have a third-party Data Provider provide the data on the CSP's behalf.
4. IPND data is used for critical purposes by the emergency call service, the emergency alert system, and national security and law enforcement agencies. It can also be used for permitted research and publication of number directories upon authorisation by the ACMA.
5. The maintenance of the IPND by the IPND Manager is supported by regulatory obligations, including:
   a. a service provider rule, which applies to CSPs (section 86 of the Act). It requires a CSP which supplies a carriage service to an end-user, where the end-user has a public number, to give the IPND Manager such information as it reasonably requires in connection with its obligation to provide and maintain the IPND (subclause 10(2) of Schedule 2 to the Act)
   b. the IPND Code, an industry code registered under Part 6 of the Act, which sets out procedures relating to the transfer of information to and from the IPND Manager and the storage of information in the IPND.
6. Further, the IPND Manager has issued the Integrated Public Number Database (IPND) Data Users and Data Providers Technical Requirements for IPND (the **Technical Requirements**) which set out information required by the IPND Manager.
7. As an industry participant to which the IPND Code applies, SMS Broadcast also has obligations under the IPND Code.
8. The IPND Code reiterates the requirement for customer data under the Technical Requirements and further sets out what, and how, customer data is to be provided to the IPND Manager (for example, setting out timeframes for provision of data to the IPND, and processes for identifying and rectifying errors in IPND data).
9. The data is defined in the IPND Code as public number customer data, or PNCD, and that term is used in this report.
10. The IPND Manager's Technical Requirements are referenced in the IPND Code, and the associated IPND Data Guideline (G619:2017) and Industry Guidance Note (IGN019) – IPND reconciliation data extract and Data Provider upload validation process.
11. Having regard to the critical uses of IPND data, and the public policy purposes to be served by relevant provisions of the Act, the Telstra Licence Conditions and the IPND Code, the ACMA considers that the IPND Manager requires PNCD from CSPs, since it is essential to the proper functioning of the IPND.
12. For the same reason, PNCD must be accurate, complete and up-to-date. An absence of, or inaccurate or incomplete, PNCD can have potential adverse impacts on the critical activities for which IPND data is used and lead to risks to individuals and public safety.

[1] Public numbers are numbers specified in the Telecommunications Numbering Plan 2015 and includes most numbers such as geographic, freephone, local rate, premium rate, and international numbers.

Compliance with the IPND service provider rule

13. Subsection 101(1) of the Act requires that service providers, including CSPs, comply with the service provider rules that apply to them. Subsection 101(3) states that subsection 101(1) is a civil penalty provision.

14. Subsection 98(1) of the Act provides that the service provider rules include those set out in Schedule 2 to the Act.

15. Clause 1 of Schedule 2 to the Act provides that service providers must comply with the Act.

16. Clause 10 of Schedule 2 requires that if a CSP supplies a carriage service to an end-user, and the end-user has a public number, the CSP must give the IPND Manager such information as it reasonably requires to fulfil its obligation to provide and maintain the IPND.

17. The ACMA has considered whether SMS Broadcast complied with the service provider rule at clause 10 of Schedule 2 to the Act by addressing the questions set out in Table 2 below.

Table 2: Assessing compliance with the service provider rule

Is SMS Broadcast a CSP?	Yes. SMS Broadcast is a CSP as defined at section 87 of the Act as it supplies carriage services to the public. Accordingly, it must comply with the service provider rules that apply to it.
Did SMS Broadcast supply the carriage services to end-users with public numbers?	Yes. SMS Broadcast supplies or supplied the carriage services under investigation to end-users with public numbers. Based on information obtained from SMS Broadcast, from 25 October 2019 to 8 June 2023, SMS Broadcast has issued 2,561 numbers to end-users and supplies or supplied the carriage services to them.
Did SMS Broadcast give the IPND Manager such information as the IPND Manager reasonably requires to provide and maintain the IPND, in relation to the carriage services?	No. On 7 July 2023, SMS Broadcast stated it had not given PNCD to the IPND. Between 25 October 2019 and 8 June 2023, SMS Broadcast failed to provide the IPND Manager information it reasonably requires to provide and maintain the IPND on 2,561 occasions.

18. Accordingly, the ACMA finds SMS Broadcast contravened subsection 101(1) of the Act on 2,561 occasions by failing to comply with the service provider rule at clause 10 of Schedule 2 to the Act.

Compliance with the IPND Code

Clause 4.2.1 – provision of PNCD to the IPND Manager

19. Clause 4.2.1 of the IPND Code provides that:

> *Each CSP that provides a Carriage Service to a Customer using a Number must provide the IPND Manager the relevant PNCD, including transaction updates [such as changes to PNCD], 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.*

20. The ACMA has considered whether SMS Broadcast complied with clause 4.2.1 of the IPND Code by addressing the questions set out in Table 3 below.

Table 3: Assessing compliance with the IPND Code upload obligation

Is SMS Broadcast a CSP?	Yes - refer to Table 2 above.
Does or did SMS Broadcast supply the carriage services to customers with public numbers?	Yes - refer to Table 2 above.
Did SMS Broadcast provide the IPND Manager the relevant PNCD, including transaction updates, for the carriage services which it supplies or supplied, that occurred on one business day, by the end of the next business day (including all transactions relating to connections or disconnections)?	No. On 7 July 2023, SMS Broadcast stated it did not provide the IPND Manager relevant PNCD within the required timeframe on 2,547 occasions for carriage services under investigation[2] which SMS Broadcast supplies or supplied. Specifically, between 20 March 2020 and 8 June 2023, SMS Broadcast failed to provide to the IPND Manager, within the required timeframe, any PNCD on 2,547 occasions.

21. Accordingly, the ACMA finds SMS Broadcast contravened clause 4.2.1 of the IPND Code on 2,547 occasions.

<u>Issue #2: Scams Code compliance</u>

Background to the Scams Code

22. The Scams Code places obligations on all C/CSPs to protect consumers from harms caused by scams and to disrupt scam activity in Australia.

23. Among the obligations, the Scams Code places requirements on C/CSPs to not originate SM traffic on their networks:

    a. using Alphanumeric Sender IDs without taking steps to confirm that the A-Party has a valid use case.

    b. where the A-Party does not hold rights of use (ROU) to the number.

24. The Scams Code also places obligations on C/CSPs to report blocked scam calls and scam SMs to the ACMA quarterly.

Compliance with the Scams Code

25. Clause 5.2.1 states:

    Originating C/CSPs must prevent carriage of SMs where the A-Party does not hold ROU to the number.

26. To determine SMS Broadcast’s compliance, the ACMA has addressed the questions set out in Table 4 below.

[2] The current investigation concerns contraventions of the current IPND Code, registered on 20 March 2020.

Table 4: Conditions for originating SMs using numbers

Is SMS Broadcast a CSP?	Yes – refer to Table 2 above. Accordingly, SMS Broadcast must comply with clause 5.2.1 of the Scams Code.
Does SMS Broadcast enable carriage of SMs on its telecommunications network using numbers?	Yes. Information provided by SMS Broadcast indicates that it enables its A-Party customers to use numbers to send SMs.
Does SMS Broadcast have processes in place to verify A-Party customers hold ROU to a number used to send a SMs.	Yes. SMS Broadcast establishes ROU by issuing numbers directly to customers or allowing customers to use “rotary” numbers held by SMS Broadcast. Where a customer uses a number issued by another provider, SMS Broadcast uses two factor authentication to verify the number at the time of account set-up.
Did SMS Broadcast prevent carriage of SMs where the A-Party did not hold ROU to the number?	Information provided by SMS Broadcast indicates that, on 10 August 2022 and on at least 16,289 occasions, it originated scam SMs where the A-Party (the initiator of the SMs, i.e. the scammer) did not hold ROU to the number used. The ACMA notes that ROU to the number was held by an SMS Broadcast customer. SMS Broadcast states that the scam SMs were sent as a result of an account take-over caused by poor security practices on the part of its customer.

27. Accordingly, the ACMA finds SMS Broadcast did not comply with clause 5.2.1 of the Scams Code on at least 16,289 occasions.

Clause 5.2.2 – improving number and Alphanumeric Sender ID accuracy

28. Clause 5.2.2 of the Scams Code states:

> *If a SM uses an Alphanumeric Sender ID, Originating C/CSPs must only originate SMs on their Telecommunications Network using an Alphanumeric Sender ID where:*
>
> *a) it does not present as a Number; and*
>
> *b) the Originating C/CSP has been provided evidence by the A-Party confirming that the A-Party has a valid use case for the Alphanumeric Sender ID.*

29. Clause 2.2 of the Scams Code states Alphanumeric Sender ID means a personalised identifier (for example, the shortened name of a business or organisation) instead of a Number.

30. The ACMA has considered whether SMS Broadcast complied with clause 5.2.2 of the Scams Code by addressing the questions set out in Table 5 below.

Table 5: Conditions for originating SMs using Alphanumeric Sender ID

Is SMS Broadcast a CSP?	Yes – refer to Table 2 above. Accordingly, SMS Broadcast must comply with clause 5.2.2 of the Scams Code.
Has SMS Broadcast originated SMs on its telecommunications network using Alphanumeric Sender IDs	Yes. Information obtained from SMS Broadcast on 7 July 2023 indicates that it allowed A-Parties to use Alphanumeric Sender IDs to send SMs originated on its telecommunications network during the period 12 July 2022 and 8 June 2023.

where it does not present as a number?	
Was SMS Broadcast provided evidence by the A-Party confirming that the A-Party had a valid use case for the Alphanumeric Sender ID?	No. Between 12 July 2022 and 8 June 2023 SMS Broadcast originated an estimated 4,588,941 SMs using Alphanumeric Sender IDs, where SMS Broadcast did not obtain evidence from the A-Party confirming it had a valid use case. Of these SMs, at least 1,240,548 were identified as scam SMs.

31. Accordingly, the ACMA finds SMS Broadcast did not comply with clause 5.2.2 of the Scams Code on an estimated 4,588,941 occasions. On at least 1,240,548 of these occasions, SMS Broadcast’s non-compliance was used by scammers to send SMS scams.