Australian Government

Australian Communications and Media Authority

Investigation Report

Summary	
Entity	NETSIP PTY LTD (**NetSIP**)
ACN	131 968 744
Type of entity	Carriage service provider (**CSP**)
Relevant legislation	*Telecommunications Act 1997* (Cth) (the **Act**) Industry Code C661:2022 Reducing Scam Calls and Scam SMs (the **Code**)
Date of findings	1 November 2024

Findings

The Australian Communications and Media Authority (**ACMA**) finds that NetSIP has contravened the Code, as set out at Table 1 below.

Table 1: Summary of contraventions

Legislation	Provision	Number of contraventions	Dates
The Code	Clause 1.1.3	At least 6 occasions	4 May, 12 June, 30 June, 3 July, 7 August and 19 September 2023
	Clause 4.2.10	At least 6 occasions	4 May, 12 June, 30 June, 3 July, 7 August and 19 September 2023
	Clause 4.3.1	At least 1 occasion	7 August 2023
	Clause 4.6.2	At least 15 occasions	3 July 2023, during March, April and May 2024
	Clause 6.1.1(a)	On 1 occasion	28 October 2022

Reasons

1. The reasons for the ACMA's findings, including key elements which establish the contraventions, are informed by:

   (a) information and documents obtained from NetSIP on 11 July 2024 under statutory notice given by the ACMA under section 521(2) of the Act dated 7 June 2024;

   (b) ACMA analysis of traceback emails made by carriers and carriage service providers (**C/CSPs**) under the Code; and

   (c) a submission from NetSIP on 1 October 2024.

Relevant background

2. The Code is an industry code registered by the ACMA under Part 6 of the Act. The Code places obligations on all C/CSPs to implement measures to protect consumers from harms caused by scams and to disrupt scam activity in Australia.
3. Among other obligations, the Code places obligations on C/CSPs to:
   (a) if notified of a material issue of alleged call line identification (CLI) spoofing that transited their network, forward details to the C/CSP from which it received the calls (with a copy to the ACMA), as soon as practicable;

   (b) monitor for scam calls;

   (c) share information about the origin and transit path of the confirmed scam calls with the ACMA; and

   (d) report scam calls blocked to the ACMA.
4. The purpose of the Code is to protect consumers from harms caused by scams by disrupting scam activity in Australia. Key elements to achieving this objective are ecosystem-wide level compliance with traceback arrangements and effective information sharing across the sector and with government.
5. The Code contains specific timing obligations that must be read in conjunction with the Industry Guideline G664:2022 Reducing Scam Calls and Scam SMS Supplementary Information (the **Guideline**).[1] These obligations include timeframes for notifications of material instances of scam calls, including to the ACMA. Adherence to these timeframes is critical to timely identification of emerging scam threats and actions by C/CSPs and government agencies to disrupt the activity.
6. The Code also places obligations on C/CSPs to report to the ACMA on a quarterly basis. This information is critical to understanding eco-system-wide scam trends, the activities of individual C/CSPs and the effectiveness of industry-wide disruption activities.
7. The ACMA investigation into NetSIP's compliance with the Code is supported by information provided by Telstra Limited (**Telstra**) and Singtel Optus Pty Limited (**Optus**) to NetSIP via traceback emails (copying in the ACMA) on 4 May, 12 June, 30 June, 3 July, 7 August and 19 September 2023.

Compliance with clause 4.2.10 – Countering CLI Spoofing

8. Clause 4.2.10 of the Code states:

   If the Notifying C/CSP provides the notification under clause 4.2.9 to a Transit C/CSP, the Transit C/CSP must, as soon as practicable, forward the details, (with a copy to the ACMA) to the C/CSP from which they received those calls.
9. Clause 4.2.9 of the Code states:

   If a C/CSP identifies a material issue of alleged CLI Spoofing in calls received from other C/CSPs, that C/CSP (the Notifying C/CSP) must raise the issue, as soon as practicable, with the Originating C/CSP or the Transit C/CSP delivering the call traffic (with a copy to the ACMA), for investigation and action to stop the alleged CLI Spoofing.
10. The Guideline includes, for the purposes of clause 4.2.9 and 4.2.10 of the Code, provisions on "a material issue of CLI Spoofing" and timeframes for "as soon as practicable".
11. The ACMA has considered NetSIP's compliance with clause 4.2.10 for the 4 May, 12 June, 30 June, 3 July, 7 August and 19 September 2023 traceback requests in **Tables 2** to **7**.

Table 2: ***4 May 2023 traceback request***

Is NetSIP a CSP?	Yes. NetSIP is a CSP as defined in the Code as it is a CSP as defined

[1] The Guideline is available for Industry participants as it contains information that could be used by scammers to try to circumvent protections.

	at section 87 of the Act. Accordingly, NetSIP must comply with clause 4.2.10 of the Code.
Did NetSIP have evidence of a material issue of alleged CLI Spoofing, under clause 4.2.9 of the Code?	Yes. On 4 May 2023, NetSIP received a notification from Telstra about a material issue of alleged CLI Spoofing, via a traceback request under clause 4.2.9 of the Code. Telstra's notification contained 13,746 call detail records from one Telstra allocated or ported CLI that entered the Telstra network from NetSIP on 3 May 2023. The ACMA considers that Telstra's notification identified a material issue of alleged CLI Spoofing in accordance with the Guideline.
Was NetSIP the Transit CSP?	On 11 July 2024, NetSIP confirmed it was a Transit CSP for each of the 13,746 calls identified by Telstra.
Did NetSIP provide details to the C/CSP from which it received those calls (cc'ing the ACMA), as soon as practicable?	No. Evidence obtained from NetSIP by the ACMA indicates that it provided the details for 13,746 calls that allegedly used a CLI spoofed number to the Originating C/CSP on 4 May 2023. The ACMA was not copied into the traceback email as required.

12. Accordingly, the ACMA finds that, in relation to the 4 May 2023 traceback request, NetSIP did not comply with clause 4.2.10 of the Code, nor did it comply with the Guideline, because it failed to copy in the ACMA when forwarding the details of alleged CLI Spoofing in 13,746 calls to the C/CSP from which it received those calls.

Table 3: ***12 June 2023 traceback request***

Is NetSIP a CSP?	Yes. See **Table 2**. Accordingly, NetSIP must comply with clause 4.2.10 of the Code.
Did NetSIP have evidence of a material issue of alleged CLI Spoofing, under clause 4.2.9 of the Code?	Yes. On 12 June 2023, NetSIP received a notification via a traceback request from Telstra about a material issue of alleged CLI Spoofing, via a traceback request under clause 4.2.9 of the Code. Telstra's notification contained 50,000 call detail records from 361 Telstra allocated or ported CLIs that entered the Telstra network from NetSIP between 5 and 9 June 2023. Telstra advised that it had received complaints from its customers that their numbers had been subject to CLI Spoofing. The ACMA considers that Telstra's notification identified a material issue of alleged CLI Spoofing in accordance with the Guideline.
Was NetSIP the Transit CSP?	On 11 July 2024, NetSIP confirmed it was a Transit CSP for each of the 50,000 calls identified by Telstra.
Did NetSIP provide details to the C/CSP from which it received those calls (cc'ing the ACMA), as soon as practicable?	No. Evidence obtained from NetSIP by the ACMA indicates that it provided the details for 50,000 calls that allegedly used 361 CLI spoofed numbers to the Originating C/CSPs on 13 June 2023. The ACMA was not copied into the traceback email as required.

13. Accordingly, the ACMA finds that, in relation to the 12 June 2023 traceback request, NetSIP did not comply with clause 4.2.10 of the Code, nor did it comply with the Guideline, because it failed to copy the ACMA when forwarding the details of alleged CLI Spoofing in 50,000 calls to the C/CSPs from which it received those calls.

Table 4: ***30 June 2023 traceback request***

Is NetSIP a CSP?	Yes. See **Table 2**. Accordingly, NetSIP must comply with clause 4.2.10 of the Code.
Did NetSIP have evidence of a material issue of alleged CLI Spoofing, under clause 4.2.9 of the Code?	Yes. On 30 June 2023, NetSIP received a notification from Optus about a material issue of alleged CLI Spoofing, via a traceback request under clause 4.2.9 of the Code. Optus' notification contained 445,830 call detail records from 253 Optus allocated or ported CLI that entered the Optus network from NetSIP between 13 and 28 June 2023. Optus advised that it had received complaints from their carrier partner that their numbers had been subject to CLI Spoofing. The ACMA considers that Optus' notification identified a material issue of alleged CLI Spoofing in accordance with the Guideline.
Was NetSIP the Transit CSP?	On 11 July 2024, NetSIP confirmed it was a Transit CSP for each of the 445,830 calls identified by Optus.
Did NetSIP provide details to the C/CSP from which it received those calls (cc'ing the ACMA), as soon as practicable?	No. Evidence obtained from NetSIP by the ACMA indicates that it provided the details 425,567 calls that allegedly used 39 alleged CLI spoofed numbers to the Originating C/CSP on 3 July 2023. The ACMA was not copied into the traceback email as required. For the remaining 20,263 calls that allegedly used 214 CLI spoofed numbers, NetSIP could not demonstrate that it provided call details to the C/CSPs from which it received those calls, nor did it notify the ACMA.

14. Accordingly, the ACMA finds that, in relation to the 30 June 2023 traceback request, NetSIP did not comply with clause 4.2.10 of the Code, nor did it comply with the Guideline, because it failed to copy the ACMA when forwarding the details of alleged CLI Spoofing in 425,567 calls to the C/CSP from which it received those calls, and it failed to forward the details of alleged CLI Spoofing in 20,263 calls (with a copy to the ACMA) to the C/CSPs from which it received those calls, as soon as practicable..

Table 5: ***3 July 2023 traceback request***

Is NetSIP a CSP?	Yes. See **Table 2**. Accordingly, NetSIP must comply with clause 4.2.10 of the Code.
Did NetSIP have evidence of a material issue of alleged CLI Spoofing, under clause 4.2.9 of the Code?	Yes. On 3 July 2023, NetSIP received a notification from Telstra about a material issue of alleged CLI Spoofing, via a traceback request under clause 4.2.9 of the Code. Telstra's notification referred to 22,462 calls from 305 Telstra allocated or ported CLIs that entered the Telstra network from NetSIP between 26 June and 2 July 2023. Telstra advised that it had received complaints from its customers that their numbers had been subject to CLI Spoofing. The ACMA considers that Telstra's notification identified a material issue of alleged CLI Spoofing in accordance with the Guideline.
Was NetSIP the Transit CSP?	On 11 July 2024, NetSIP confirmed it was a Transit CSP for each of the 22,462 calls identified by Telstra.
Did NetSIP provide details to the C/CSP from which it received those calls (cc'ing the ACMA), as soon as practicable?	No. Evidence obtained from NetSIP by the ACMA indicates that it provided details of 1,989 calls that allegedly used 88 CLI spoofed numbers to the Originating C/CSPs on 5 July 2023. The ACMA was not copied into the traceback email as required. For the remaining 20,473 calls that allegedly used 217 CLI spoofed numbers, NetSIP could not demonstrate that it provided call details to the C/CSP(s) from which it received those calls, nor did it notify the ACMA.

15. Accordingly, the ACMA finds that, in relation to the 3 July 2023 traceback request, NetSIP did not comply with clause 4.2.10 of the Code, nor did it comply with the Guideline, because it failed to copy the ACMA when forwarding the details of alleged CLI Spoofing in 1,989 calls to the C/CSPs from which it received those calls, and it failed to forward the details of alleged CLI Spoofing in 20,473 calls (with a copy to the ACMA) to the C/CSP(s) from which it received those calls, as soon as practicable..

Table 6: ***7 August 2023 traceback request***

Is NetSIP a CSP?	Yes. See **Table 2**. Accordingly, NetSIP must comply with clause 4.2.10 of the Code.
Did NetSIP have evidence of a material issue of alleged CLI Spoofing, under clause 4.2.9 of the Code?	Yes. On 7 August 2023, NetSIP received a notification from Telstra about a material issue of alleged CLI Spoofing, via a traceback request under clause 4.2.9 of the Code. Telstra's notification referred to 6,136 calls from 285 Telstra allocated or ported CLIs that entered the Telstra network from NetSIP between 31 July and 6 August 2023. Telstra advised that it had received complaints from its customers that their numbers had been subject to CLI Spoofing. The ACMA considers that Telstra's notification identified a material issue of alleged CLI Spoofing in accordance with the Guideline.
Was NetSIP the Transit CSP?	On 11 July 2024, NetSIP confirmed it was a Transit CSP for each of the 6,136 calls identified by Telstra.
Did NetSIP provide details to the C/CSP from which it received those calls (cc'ing the ACMA), as soon as practicable?	No. Evidence obtained from NetSIP by the ACMA indicates that it failed to analyse and provide details of 6,136 calls that allegedly used 285 CLI spoofed numbers to the C/CSPs from which it received those calls, nor did it notify the ACMA.

16. Accordingly, the ACMA finds that, in relation to the 7 August 2023 traceback request, NetSIP did not comply with clause 4.2.10 of the Code, nor did it comply with the Guideline, because it failed to forward the details of alleged CLI Spoofing in 6,136 calls (with a copy to the ACMA) to the C/CSPs from which it received those calls, as soon as practicable.

Table 7: ***19 September 2023 traceback request***

Is NetSIP a CSP?	Yes. See **Table 2**. Accordingly, NetSIP must comply with clause 4.2.10 of the Code.
Did NetSIP have evidence of a material issue of alleged CLI Spoofing, under clause 4.2.9 of the Code?	Yes. On 19 September 2023, NetSIP received a notification from Telstra about a material issue of alleged CLI Spoofing, via a traceback request under clause 4.2.9 of the Code. Telstra's notification referred to 9,669 calls from 6,760 Telstra allocated or ported CLIs that entered the Telstra network from NetSIP on 18 September 2023. The ACMA considers that Telstra's notification identified a material issue of alleged CLI Spoofing in accordance with the Guideline.
Was NetSIP the Transit CSP?	On 11 July 2024, NetSIP confirmed it was a Transit CSP for each of the 9,669 calls identified by Telstra, and those calls were from 24 customers including 20 Originating CSPs and four direct customers. The ACMA is of the view that NetSIP was the Transit CSP for calls received from 21 CSPs/customers, and the Originating CSP for calls received from three direct customers.
Did NetSIP provide details to the C/CSP from which it received those calls (cc'ing the ACMA), as soon as practicable?	No. Evidence obtained from NetSIP by the ACMA indicates it provided details of at least some of the 9,669 calls to the C/CSPs from which NetSIP received calls, however, NetSIP did not notify the ACMA.

17. Accordingly, the ACMA finds that, in relation to the 19 September 2023 traceback request, NetSIP did not comply with clause 4.2.10 of the Code, nor did it comply with the Guideline, because it failed to copy the ACMA when forwarding the details of alleged CLI Spoofing in approximate 9,669 calls to the C/CSPs from which it received those calls.

Compliance with clause 1.1.3 – Guideline

18. Clause 1.1.3 of the Code states:

    The Code should be read in conjunction with CA G664:2022 and where the G664 Guideline sets out timeframes for actions, C/CSPs must adhere to these timeframes.

19. By not meeting the timeframes set out in the Guideline for clauses 4.2.10, the ACMA finds that NetSIP has also contravened clause 1.1.3 of the Code on at least 6 occasions in relation to each of the traceback requests in Tables 2 to 7.

Compliance with clause 4.3.1 – Monitoring for Scam Calls

20. Clause 4.3.1(b) of the Code states:

    C/CSPs must monitor their networks for Scam Calls based upon; […] *(b) the CLI notified by other C/CSPs or from relevant government agencies which are associated with potential scam calls.*

Table 8: ***7 August 2023 traceback request***

Is NetSIP a CSP?	Yes. **See Table 2**. Accordingly, NetSIP must comply with clause 4.3.1(b) of the Code.
Did NetSIP monitor their networks for Scam Calls based upon the CLI notified by other C/CSPs?	No. On 7 August 2023, NetSIP received a notification from Telstra about a material issue of alleged CLI Spoofing, via a traceback request under clause 4.2.9 of the Code. Telstra's notification referred to 6,136 calls from 285 Telstra allocated or ported CLIs that entered the Telstra network from NetSIP between 31 July and 6 August 2023. NetSIP advised that it did not analyse the calls from the 200-300 unique source CLIs. The ACMA is of the view that NetSIP did not take action to monitor their networks for Scam Calls based upon the CLIs notified by Telstra on 7 August 2023.

21. Accordingly, the ACMA finds that, in relation to the 7 August 2023 traceback request, NetSIP did not comply with clause 4.3.1(b) of the Code because it failed to monitor their networks for Scam Calls based upon the CLIs notified by other C/CSP.

Compliance with clauses 4.6.2 – Exchanging information about confirmed Scam Calls

22. Clause 4.6.2 of the Code states:

    Where Scam Calls are confirmed, each C/CSP in the transit path must:
    (a) share information about the origin of the Scam Calls (including where possible the CLI of the A-Party) with the ACMA via agreed electronic means as per the template in Appendix B; and
    (b) provide details about the transit path of the Scam Calls (including, where possible, the CLI of the A-Party) to relevant government agencies via agreed electronic means, as per the template in Appendix B

23. The ACMA has considered NetSIP's compliance with clause 4.6.2 in relation to confirmed Scam Calls in **Tables 9** to **10**.

Table 9: ***3 July 2023 traceback request***

Is NetSIP a CSP?	Yes. **See Table 2**. Accordingly, NetSIP must comply with clause 4.6.2 of the Code.

Have Scam Calls been confirmed?	Yes. On 11 July 2024, NetSIP stated that Scam Calls have been confirmed in relation to a 3 July 2023 traceback request from Telstra to NetSIP.
Has NetSIP shared information about the origin and transit path of the Scam Calls (including where possible the CLI of the A-Party) with the ACMA via agreed electronic means as per the template in Appendix B of the Code?	No. Evidence obtained from NetSIP by the ACMA on 11 July 2024 indicates that NetSIP did not share information about the origin or transit path of the Scam Calls with the ACMA via agreed electronic means, as per the template in Appendix B of the Code in relation to the 3 July 2023 traceback request.

24. Accordingly, the ACMA finds that, in relation to the 3 July 2023 traceback request, NetSIP did not comply with clause 4.6.2 of the Code because it failed to share information about the origin and transit path of the confirmed Scam Calls with the ACMA, as per the template in Appendix B of the Code.

Table 10: ***March to June 2024 traceback requests***

Is NetSIP a CSP?	Yes. **See Table 2**. Accordingly, NetSIP must comply with clause 4.6.2 of the Code.
Have Scam Calls been confirmed?	Yes. On 11 July 2024, NetSIP stated that it had received notifications of material issues of alleged Scam Calls between 7 March to 7 June 2024. NetSIP further stated Scam Calls have been confirmed in relation to some of the notifications.
Has NetSIP shared information about the origin and transit path of the Scam Calls (including where possible the CLI of the A-Party) with the ACMA via agreed electronic means as per the template in Appendix B of the Code?	No. Evidence obtained from NetSIP by the ACMA on 11 July 2024 indicates that NetSIP did not share information about the origin and transit path of the Scam Calls with the ACMA via agreed electronic means as per the template in Appendix B of the Code in relation to the following traceback requests: - 6 March 2024 case no. 1500724 from Telstra - 13 March 2024 case no. 1506491 from NetSIP - 15 March 2024 case no. 1507126 from Optus - 18 March 2024 case no. 1507939 from Telstra - 21 March 2024 case no. 1506791 from Telstra - 21 March 2024 case no. 1509097 from Telstra - 9 April 2024 case no. 1517280 from TPG - 9 April 2024 case no. 1517294 from Pivotel - 11 April 2024 case no. 1521131 from Telstra - 12 April 2024 case no. 1521313 from Optus - 17 April 2024 case no. 1525447 from Optus - 17 April 2024 case no. 1525626 from Symbio - 26 April 2024 case no. 1528761 from Optus - 23 May 2024 case no. 1542246 from Symbio.

25. Accordingly, the ACMA finds that, in relation to the traceback request 3 July 2023 and a further 14 traceback requests during March, April and May 2024, NetSIP did not comply with clause 4.6.2 of the Code because it failed to share information about the origin and transit path of the confirmed Scam Calls with the ACMA, as per the template in Appendix B of the Code.

Compliance with clause 6.1.1(a) – Reporting

26. Clause 6.1.1(a) of the Code states:

    C/CSPs must, within 20 Business Days of the end of each calendar quarter, report to the ACMA:

    (a) For Scam Calls, in the format and detail specified in Appendix D.

27. Appendix D of the Code requires C/CSPs to report the total number of Sam Calls blocked during the calendar quarter, as well as a breakdown of the scam call types.

28. To determine NetSIP's compliance, the ACMA has addressed the questions set out in **Table 11** below.

Table 11: Reporting obligations

Is NetSIP a CSP?	Yes. **See Table 2**. Accordingly, NetSIP must comply with clause 6.1.1(a) of the Code.
Did NetSIP, within 20 Business Days of the end of each quarter since the code commenced in July 2022, report to the ACMA the number of scam calls it blocked, in the format and detail specified in Appendix D of the Code?	No. The ACMA did not receive reports from NetSIP about the number of Scam Calls it blocked for the July to September 2022 quarter within the requisite timeframe. Accordingly, NetSIP did not meet the requirement for provision of the detail specified by Appendix D of the Code for the quarter between July to September 2022.

29. Accordingly, the ACMA finds that NetSIP has not complied with clause 6.1.1(a) of the Code on one occasion.