

Investigation Report

Summary	
Entity	TeleSign Corporation (ABN 62 319 066 528)
Type of entities	Carriage service provider (CSP)
Relevant legislation	<i>Telecommunications Act 1997</i> (Cth) (the Act) Industry Code C661:2022 Reducing Scam Calls and Scam SMs (the Code)
Date of findings	20 February 2025, amended 9 April 2025 due to additional information provided by Telesign.

Findings

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

Table 1: Summary of contraventions

Legislation	Provision	Number of contraventions	Relevant Dates
The Code	Subclause 1.1.3	19	4, 5 and 6 November 2023 5, 8 and 21 February 2024 7 and 25 May 2024 4, 6 and 24 June 2024 2, 3, 7 (2 occasions), 11, 17, 21 and 23 July 2024
	Subclause 5.2.4	17	4, 5 and 6 November 2023 5, 8 and 21 February 2024 7 and 25 May 2024 24 June 2024 2, 3, 7 (2 occasions), 11, 17, 21 and 23 July 2024
	Subclause 5.2.7	2	4 and 6 June 2024
	Subclause 6.1.1	8	21 days after the end of each quarter from July 2022 to June 2024.

Reasons

- The reasons for the ACMA's findings, including key elements which establish the contraventions, are informed by:
 - information and documents obtained from TeleSign under statutory notice given by the ACMA under section 521(2) of the Act dated 5 August 2024, and
 - ACMA analysis of traceback emails made by carriers and CSPs (**C/CSPs**) under the Code.

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 an alleged misuse of an Alphanumeric Sender ID, forward the details, to the C/CSP from which they received those SMs (with a copy also provided to the ACMA)
 - (b) if the alleged Scam SMs using an Alphanumeric Sender ID are found not to be Scam SMs, share the details with other relevant CSPs and the ACMA
 - (c) report Scam Calls and Scam SMs blocked to the ACMA.
4. The purpose of the Code is to protect consumers from harms caused by scams by disrupting scam activities in Australia. Key elements to achieving this objective are network-wide level compliance with traceback arrangements and effective information sharing across the sector and with government agencies.
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**). These obligations include timeframes for notifications of material instances of Scam SMs, 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 scam activities.
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, threats to consumers and the effectiveness of industry-wide disruption activities.
7. The ACMA investigation into TeleSign's compliance with the Code is supported by information provided by the Notifying CSP to TeleSign via traceback emails (copying in the ACMA) on 4, 5 and 6 November 2023, 5, 8 and 21 February 2024 and additional traceback requests between May to July 2024 as provided by TeleSign.

Compliance with subclause 5.2.4 – sharing information about material misuse of an Alphanumeric Sender ID

8. Subclause 5.2.3 of the Code states:

If a C/CSP identifies what it believes is a material misuse of an Alphanumeric Sender ID, 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 SMs (with a copy to the ACMA), for investigation and action to stop the alleged misuse of the Alphanumeric Sender ID.
9. Subclause 5.2.4 of the Code states:

If the Notifying C/CSP provides the notification under subclause 5.2.3 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 SMs.
10. The ACMA has considered TeleSign's compliance with subclause 5.2.4 for the November 2023, February 2024 and May to July 2024 traceback requests in **Tables 2 to 6** below.

Table 2: 4, 5 and 6 November 2023 traceback requests

Is TeleSign a CSP?	Yes. TeleSign is a CSP as defined in the Code as it is a CSP as defined at section 87 of the Act. Accordingly, TeleSign must comply with subclause 5.2.4 of the Code.
Did TeleSign have evidence of a material misuse of an Alphanumeric Sender ID, under subclause 5.2.3 of the	Yes. TeleSign received three notifications from a Notifying CSP, one each on 4, 5 and 6 November 2023, via a traceback request. The traceback requests relate to 9,668 SMs with malicious contents that had the same Alphanumeric Sender ID sent from a TeleSign allocated CLI that entered the Notifying CSP's network on 4, 5 and 6 November

Code?	2023. The ACMA considers that each of the notifications identified a material misuse of an Alphanumeric Sender ID under subclause 5.2.3.
Was TeleSign the Transit CSP?	On 1 September 2024, TeleSign confirmed it was a Transit CSP for each of the 9,668 SMs identified by the Notifying CSP.
Did TeleSign provide details to the C/CSP from which it received those SMs (cc'ing the ACMA), as soon as practicable?	No. TeleSign stated that it investigated the alleged scam traffic including reaching out to Entity A from which TeleSign received the SMs. TeleSign provided screenshots of their communication with Entity A. The evidence indicates that TeleSign did not copy in the ACMA when forwarding Entity A the details of the 9,668 alleged Scam SMs for the 4, 5 & 6 November notifications.

Table 3: 5 February 2024 traceback request

Is TeleSign a CSP?	Yes. See Table 2 . Accordingly, TeleSign must comply with subclause 5.2.4 of the Code.
Did TeleSign have evidence of a material misuse of an Alphanumeric Sender ID, under subclause 5.2.3 of the Code?	Yes. TeleSign received a notification from a Notifying CSP on 5 February 2024, via a traceback request. The traceback request relates to 1,121 SMs with malicious contents that had the same Alphanumeric Sender ID sent from a TeleSign allocated CLI that entered the Notifying CSP's network on 1 February 2024. The ACMA considers that the notification identified a material misuse of an Alphanumeric Sender ID under subclause 5.2.3.
Was TeleSign the Transit CSP?	On 1 September 2024, TeleSign confirmed it was a Transit CSP for each of the 1,121 SMs identified by the Notifying CSP.
Did TeleSign provide details to the C/CSP from which it received those SMs (cc'ing the ACMA), as soon as practicable?	No. TeleSign stated that it investigated the alleged scam traffic including reaching out to Entity B from which TeleSign received the SMs. TeleSign provided screenshots of their internal and external communications which indicate that TeleSign did not copy in the ACMA when forwarding Entity B the details of the 1,121 alleged Scam SMs in the 5 February notification.

Table 4: 8 February 2024 traceback request

Is TeleSign a CSP?	Yes. See Table 2 . Accordingly, TeleSign must comply with subclause 5.2.4 of the Code.
Did TeleSign have evidence of a material misuse of an Alphanumeric Sender ID, under subclause 5.2.3 of the Code?	Yes. TeleSign received a notification from a Notifying CSP on 8 February 2024, via a traceback request. The traceback request relates to 380 SMs with malicious contents that had the Alphanumeric Sender ID sent from a TeleSign allocated CLI that entered the Notifying CSP's network on 8 February 2024. The ACMA considers that the notification identified a material misuse of an Alphanumeric Sender ID under subclause 5.2.3.
Was TeleSign the Transit CSP?	On 1 September 2024, TeleSign confirmed it was a Transit CSP for each of the 380 SMs identified by the Notifying CSP.
Did TeleSign provide details to the C/CSP from which it received those SMs (cc'ing	No. TeleSign stated that it investigated the alleged scam traffic including

the ACMA), as soon as practicable?	reaching out to Entity C from which TeleSign received the SMs. TeleSign provided screenshots of their communication with Entity C. The ACMA did not receive any copy of the notification. The evidence indicates that TeleSign did not copy in the ACMA when forwarding Entity C the details of the 380 alleged Scam SMs in the 8 February notification.
------------------------------------	---

Table 5: 21 February 2024 traceback request

Is TeleSign a CSP?	Yes. See Table 2 . Accordingly, TeleSign must comply with subclause 5.2.4 of the Code.
Did TeleSign have evidence of a material misuse of an Alphanumeric Sender ID, under subclause 5.2.3 of the Code?	Yes. TeleSign received a notification from a Notifying CSP on 21 February 2024, via a traceback request. The traceback request relates to 43 SMs with malicious contents and multiple Alphanumeric Sender IDs, sent from a TeleSign allocated CLI that entered the Notifying CSP's network between 18 and 21 February 2024. The ACMA considers that the notification identified material misuse of multiple Alphanumeric Sender IDs under subclause 5.2.3.
Was TeleSign the Transit CSP?	On 1 September 2024, TeleSign confirmed it was a Transit CSP for each of the 43 SMs identified by the Notifying CSP.
Did TeleSign provide details to the C/CSP from which it received those SMs (cc'ing the ACMA), as soon as practicable?	No. TeleSign stated that it investigated the alleged scam traffic including reaching out to Entities C, D and E, from which TeleSign received the SMs. TeleSign provided screenshots of their communication with the three entities. The ACMA did not receive any copy of the notifications. The evidence indicates that TeleSign failed to copy in the ACMA when forwarding the three entities the details of the 43 alleged Scam SMs in the 21 February notification.

Table 6: May to July 2024 traceback requests

Is TeleSign a CSP?	Yes. See Table 2 . Accordingly, TeleSign must comply with subclause 5.2.4 of the Code.
Did TeleSign have evidence of a material misuse of an Alphanumeric Sender ID, under subclause 5.2.3 of the Code?	Yes. TeleSign received 17 notifications from a Notifying CSP between 7 May and 23 July 2024, via traceback requests. The traceback requests relate to SMs with malicious contents and various Alphanumeric Sender IDs sent from TeleSign allocated CLIs that entered the Notifying CSP's network. The ACMA considers that each of the notifications identified a material misuse of an Alphanumeric Sender ID under subclause 5.2.3.
Was TeleSign the Transit CSP?	On 20 January 2025, TeleSign provided evidence that it was a Transit CSP for each of the SMs identified by the Notifying CSP.
Did TeleSign provide details to the C/CSP from which it received those SMs (cc'ing the ACMA), as soon as practicable?	No. TeleSign provided screenshots of their communication with the entities from which TeleSign received the SMs, including Entities B, E and F. The evidence indicates that TeleSign did not forward the details of the alleged Scam SMs to the CSPs delivering the SMs in response to the following 2 notifications: <ul style="list-style-type: none"> • 25 May 2024: case no. 825245 • 7 July 2024: case no. 844317.

	<p>Further, the evidence (including ACMA record-searches) indicates that TeleSign did not copy in the ACMA when forwarding the details of the alleged Scam SMSs to the CSPs delivering the SMSs for the following 9 notifications:</p> <ul style="list-style-type: none"> • 7 May 2024: case no. 817035 • 24 June 2024: case no 838596 • 2 July 2024: case no. 841930 • 3 July 2024: case no. 842560 • 7 July 2024: case no. 844285 • 11 July 2024: case no. 845993 • 17 July 2024: case no. 848742 • 21 July 2024: case no. 850121 • 23 July 2024: case no. 850942.
--	---

11. Accordingly, the ACMA finds that on a total of 17 occasions, TeleSign did not comply with subclause 5.2.4 of the Code, nor did it comply with the Guideline because it failed to:

- (a) as soon as practicable, for the notifications on 25 May and 7 July 2024, forward the details of alleged Scam SMSs (with a copy to the ACMA) to the C/CSPs from which it received those SMSs; and
- (b) failed to copy in the ACMA for the notifications on 4, 5, 6 November 2023, 5, 8 and 21 February 2024 and another 9 notifications in May to July 2024 when forwarding the details of alleged Scam SMSs to the C/CSPs from which it received those SMSs.

Compliance with subclause 5.2.7 – Sharing information about alleged Scam SMSs found not to be Scam SMSs

12. Subclause 5.2.7 of the Code states:

If the alleged Scam SMSs using an Alphanumeric Sender ID notified under subclause 5.2.3 are found not to be Scam SMSs the Originating C/CSP or Transit C/CSP must provide details about the SMSs to the adjacent Transit C/CSPs and Notifying C/CSPs, as soon as practicable, via agreed electronic means (with a copy to the ACMA).

13. The ACMA has considered TeleSign's compliance with subclause 5.2.7 for the 4 and 6 June 2024 traceback requests in **Table 7**.

Table 7: 4 and 6 June 2024 traceback requests

Is TeleSign a CSP?	<p>Yes. See Table 2.</p> <p>Accordingly, TeleSign must comply with subclause 5.2.7 of the Code.</p>
Did TeleSign find any alleged Scam SMSs using an Alphanumeric Sender ID not to be Scam SMSs?	<p>Yes.</p> <p>Yes. TeleSign received two notifications from a Notifying CSP between 4 and 6 June 2024, via traceback requests. The traceback requests relate to alleged Scam SMSs with a sender ID associated with a well-known Australian brand sent from TeleSign allocated CLIs that entered the Notifying CSP's network.</p> <p>TeleSign investigated the alleged Scam SMSs and found them to be legitimate SMSs from an international brand incorrectly sent to wrong recipients.</p>
Was TeleSign the Transit CSP?	<p>On 20 January 2025, TeleSign provided evidence that it was a Transit CSP for each of the SMSs identified by the Notifying CSP.</p>
Did TeleSign provide details of the SMSs to the Notifying C/CSP from which it received those SMSs (cc'ing the	<p>No.</p> <p>TeleSign did not copy the ACMA when providing details to the Notifying CSP about the SMSs found not to be Scam SMSs.</p>

ACMA), as soon as practicable?	
--------------------------------	--

14. Accordingly, the ACMA finds that, in relation to the alleged Scam SMs referred to in the 4 and 6 June 2024 traceback requests, on 2 occasions, TeleSign did not comply with subclause 5.2.7 of the Code because it failed to, as soon as practicable, copy in the ACMA when providing details to the Notifying CSP about the alleged Scam SMs found not to be Scam SMs.

Compliance with subclause 1.1.3 – Guideline

15. Subclause 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.
16. By not meeting the timeframes set out in the Guideline for subclause 5.2.4, the ACMA finds that TeleSign has also contravened subclause 1.1.3 of the Code on 17 occasions in relation to each of the traceback requests in Tables 2 to 6.
17. By not meeting the timeframes set out in the Guideline for subclause 5.2.7, the ACMA finds that TeleSign has also contravened subclause 1.1.3 of the Code on 2 occasions in relation to the traceback requests in Table 7.

Compliance with subclause 6.1.1 – Reporting

18. Subclause 6.1.1 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.
(b) For Scam SMs, in the format and detail specified in Appendix E.
19. Appendix D and E of the Code requires C/CSPs to report the total number of Scam Calls and Scam SMs blocked respectively during the calendar quarter, as well as a breakdown of the Scam Call and Scam SMs types.
20. To determine TeleSign's compliance, the ACMA has addressed the questions set out in **Table 8** below.

Table 8: Reporting obligations

Is TeleSign a CSP?	Yes. See Table 2. Accordingly, TeleSign must comply with subclause 6.1.1(a) and (b) of the Code.
Did TeleSign, 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, and the number of Scam SMs, it blocked, in the format and detail specified in Appendix D and, E respectively, of the Code?	No. The ACMA did not receive reports from TeleSign about the number of Scam Calls or Scam SMs it blocked between July to September 2022 quarter and the April to June 2024 quarter, within the requisite timeframes. Accordingly, TeleSign did not meet the requirement for provision of the details specified by Appendix D and E of the Code for each quarter between July 2022 to June 2024.

21. Accordingly, the ACMA finds that TeleSign has not complied with subclause 6.1.1(a) and (b) of the Code on 8 occasions because it failed to provide required blocking details within 20 days of the end of each calendar quarter between July 2022 to June 2024.