Australian Government | acma

Australian Communications and Media Authority

Investigation report

Summary	
Entity	Telstra Limited (**Telstra**) including Belong, a Division of Telstra
Australian Company Number	ACN 086 174 781
Type of entity	Carriage service provider (**CSP**)
Relevant Legislation	• *Telecommunications Act 1997* (the **Act**) • *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* (the **Determination**)
Date	4 June 2026

Findings

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

Table 1: Summary of contraventions

Regulation	Provision	Number of contraventions	Relevant Period
The Act	Subsection 101(1)	28	10 January to 30 October 2025
The Determination	Section 8	15	10 January to 30 October 2025
	Subsection 13(1)	13	13 February to 27 October 2025

Reasons

1. The reasons for the ACMA's findings, including the key elements which establish the contraventions, are based on:
    a. mobile number fraud (**MNF**) intelligence relating to Telstra, including its Belong division, obtained by the ACMA between 1 January 2025 and 31 July 2025,
    b. information obtained from Telstra on 21 November 2025, 5 and 19 December 2025, 30 January and 25 February 2026 in response to a Statutory Notice given to it under section 521 of the Act and the ACMA's requests for further information,
    c. Telstra's response to the preliminary findings on 26 March 2026, and
    d. additional information obtained from Telstra on 2 April 2026, 7 April 2026 and 19 June 2026.

Background

2. The objectives of the Determination are to:
    a. reduce the harm caused to customers when access to their personal information, business information or telecommunications service is targeted by unauthorised persons or entities; and
    b. require Carriage Service Providers (CSPs) to follow effective identity authentication processes to protect the security of high-risk customer interactions (**Interactions**[1]).

[1] An interaction is between a CSP and a requesting person, in relation to a customer's telecommunications service, initiated by either the requesting person or by the CSP, during which one or more HRCTs are requested.

3. The Determination is a service provider determination that commenced on 30 June 2022 and applies to CSPs:
    a. involved in the supply of a telecommunications service; and
    b. when conducting a high-risk customer interaction relating to a customer of a CSP.[2]
4. The Determination requires that the CSP, prior to undertaking the first high-risk customer transaction[3] (**HRCT**) during an interaction, use identity authentication processes to authenticate that the person requesting the transaction is the customer (or their authorised representative) for that service.

Compliance with the Determination

5. The Determination is a service provider determination made under subsection 99(1) of the Act.
6. Subsection 101(1) of the Act requires that service providers, including CSPs, comply with the service provider rules that apply to them. Paragraph 98(1)(b) of the Act provides that service provider determinations in force under section 99 are service provider rules. Accordingly, CSPs must comply with the Determination.

Section 8 - Requirement to confirm the requesting person is the customer or the customer's authorised representative

7. Section 8 of the Determination requires that, prior to undertaking the first HRCT during an Interaction, a CSP must confirm that the person requesting a high-risk transaction is the customer or the customer's authorised representative, using an applicable identity authentication process, specified under sections 9, 10 or 11 of the Determination.
8. An identity authentication process means a process described in subsections 9(1), 9(2), 9(3), 10(2) or 11(2) of the Determination.
9. The ACMA has considered whether Telstra complied with section 8 of the Determination at Table 2 below.

Table 2: Assessing compliance with section 8

Is Telstra a CSP who provides telecommunications services to customers?	Yes. Telstra 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 Telstra complete HRCTs during the investigated period 1 January to 7 November 2025	Yes. Based on information provided by Telstra it completed interactions (which included interactions from the Belong division) across both assisted (i.e. via call centres and messaging) and unassisted (i.e. via digital self-service) channels for the period 1 January to 7 November 2025. Under the Determination, SIM swap requests and changes to a customer's personal or account security information are HRCTs. During each interaction, at least one HRCT was completed.
Prior to undertaking the first HRCT in the course of an Interaction, did Telstra confirm the requesting person was the customer, or the customer's authorised representative, for the service by use of	No, not in some cases. Based on information obtained from Telstra, between 10 January and 30 October 2025 Telstra did not comply with the required authentication processes under subsection 9(3) of the Determination for: • 12 interactions via its customer contact centres (phone and messaging). These consisted of:

[2] The Determination does not apply to a customer who is an account managed customer or an integrated customer.
[3] 'High-risk customer transaction' is defined in section 6 of the Determination.

the identity authentication process or processes in section 9?	○ 8 instances where an agent made outbound calls to an unlisted contact number on the account; ○ 2 instances where the agent proceeded with the HRCT without completing MFA; and ○ 2 instances where an unknown actor created a fraudulent duplicate customer account and completed MFA through newly added details associated with that account. Telstra stated that through social engineering, the unknown actor in each case was able to request the agent to make unauthorised changes to the customers' actual accounts without authentication. • 2 Interactions via Telstra's retail stores. In one case, an agent incorrectly verified a date of birth, and in the second case the agent failed to perform MFA prior to undertaking the HRCT.
Where section 10 applied, prior to undertaking the first HRCT in the course of an Interaction, did Telstra confirm the requesting person was the customer, or the customer's authorised representative, for the service by use of the identity authentication process or processes in section 10?	No. During an interaction on 29 August 2025, Telstra did not comply with the required authentication process provided under subsection 10(2) of the Determination. Telstra stated that only one unique government document was provided by the customer for the identity verification process using DVS. Two unique government documents are required under subsection 10(3) to confirm the identity of the customer using this process. Therefore, Telstra did not comply with the identity authentication process under section 10 of the Determination for one interaction.

10. Accordingly, the ACMA finds that Telstra has contravened section 8 of the Determination on 15 occasions in the period between 10 January and 30 October 2025.

Section 13 – requirements to provide fraud mitigation protections

11. Subsection 13(1) requires a CSP to have systems in place to identify customers who are at risk of fraud in relation to their telecommunications service and to provide those customers with fraud mitigation protections.

12. The ACMA has considered whether Telstra complied with subsection 13(1) of the Determination at Table 3 below.

Table 3: Assessing compliance with subsection 13(1)

Is Telstra a CSP who provides telecommunications services to customers?	Yes. Refer to Table 3 above. Accordingly, Telstra must comply with the service provider rules that apply to it.
Did Telstra have systems in place to identify customers who were at risk of fraud in relation to their telecommunications service?	Yes. Telstra has provided information that it maintains systems to identify customers at risk of fraud, including a range of monitoring, detection and account-flagging measures, with suspected cases escalated to specialised fraud and high-risk teams for further assessment and remediation. This is supported by fraud identification and escalation procedures across Telstra and Belong, as well as staff training modules covering authentication and fraud prevention.

Did Telstra provide customers identified at risk of fraud in relation to their telecommunication service with fraud mitigation protections?	No, not in some cases. Based on information provided by Telstra, there were 13 instances between 13 February 2025 and 27 October 2025 where customers raised concerns with Telstra or Belong they were at risk of fraud in relation to their telecommunications service. During these interactions Telstra or Belong either did not identify the customers as being at risk in line with their own systems and procedures and therefore fraud mitigation protections were not provided, or identified customers as being at risk of fraud but did not apply appropriate fraud mitigation protections. These interactions consisted of: Telstra • 2 instances on 26 June and 14 July 2025 where despite being informed by the customer of the receipt of an unsolicited UVC associated with Telstra, the Telstra agent did not identify that the customer was at risk of fraud and subsequently did not provide them with fraud mitigation protections. • 6 instances between 13 February and 27 October 2025, in which customers were identified as being at risk of fraud, but Telstra did not provide fraud mitigation protections. This included instances where processes to implement the protection were not adhered to or actioned by the Telstra agent, thereby compromising the intended measure and resulting in fraud occurring. Belong • 1 instance on 27 May 2025 where a fraud mitigation measure was eventually provided, however this was not provided at the time the customer identified that they were at risk and was only applied after a subsequent unauthorised SIM swap had occurred. • 2 instances on 6 March and 26 August 2025, where the customers were identified as being at risk of fraud, but Belong did not provide fraud mitigation protections. This included instances where processes to implement the protection were not adhered to or actioned by the Belong agent, thereby compromising the intended measure and resulting in fraud occurring. • 2 instances where a Belong customer, who had recently had fraud mitigation protections temporarily applied to their account following receipt of an unsolicited UVC, made further reports regarding the receipt of additional UVCs that they did not initiate, consisting of: ○ A first instance on 10 June 2025 where the Front of House agent did not provide measures in accordance with Belong's policy to reopen or escalate the case of this type, instead suggesting the customer change their account password. ○ A second instance on 13 June 2025 where the customer reported an unauthorised SIM order on their account. While a High-Risk Privacy and Fraud case was raised, and Belong's Enhanced Customer Care team validated the email and

	contact phone number on the account, a block on further SIM swaps was not enacted in accordance with Belong's policy. Subsequently, an unauthorised SIM swap occurred on 16 June 2025. **Telstra's submissions** Telstra submitted that it did provide fraud mitigation protections as required under paragraph 13(1)(b) to customers in relation to 6 of the 15 interactions. For each of these interactions, Telstra stated that its retrospective review indicated that customers were either provided with appropriate fraud mitigation protections including the stopping of high-risk transactions, or that there were no objective indicators of fraud present at the time of the interaction. The ACMA accepts Telstra's submission that it provided fraud mitigations in relation to two of the interactions. The ACMA notes however, that in relation to the remaining 4 interactions, the fraud mitigation protections listed by Telstra were either not provided prior to the unauthorised SIM swap occurring when clear indicators of fraud risk were first identified in line with its own systems and procedures, or, where protections were applied in response to an indicator of fraud, they were not implemented in accordance with Telstra's own processes, resulting in the unauthorised SIM swap still occurring.

13. Accordingly, the ACMA finds that Telstra has contravened subsection 13(1) of the Determination on 13 occasions in the period between 13 February 2025 and 27 October 2025.

Compliance with the Act

14. The Determination is a service provider determination made under subsection 99(1) of the Act and thereby, a service provider rule in accordance with paragraph 98(1)(b). Given subsection 101(1) of the Act requires CSPs to comply with the service provider rules, non-compliance with the Determination is a contravention of the Act.

15. Accordingly, the ACMA finds that by having contravened section 8 and subsection 13(1) of the Determination as set out above, Telstra also contravened subsection 101(1) of the Act[4] on 28 occasions.

[4] Subsection 101(3) of the Act provides that subsection 101(1) of the Act is a civil penalty provision.