

SMS Sender ID Register

Key Compliance and Readiness Checklist: Originating Telco

- All references refer to the [Telecommunications \(SMS Sender ID register\) Industry Standard 2025](#) unless otherwise stated.
- This checklist is not exhaustive and should not be considered as legal advice. Compliance is the responsibility of the provider.
- An Australian Electronic Messaging Service Provider (EMSP) may choose to fulfill some or all of its obligations by partnering with another participating telco, as per Section 4 of the Standard.

SYSTEMS READINESS

1. Compliance obligations are understood.
2. All systems and processes have been tested to ensure they will perform and meet compliance obligations from 1 July 2026.

PARTICIPATION, POLICIES AND PROCEDURES

3. Approval to participate in the Sender ID Register as an Originating telco has been applied for, and received, under section 484F of the [Telecommunications Act 1997](#).
4. Policies and procedures to comply with **ALL** applicable obligations have been implemented, as per Section 19 of the Standard.
5. Policies and procedures to deal with, record and resolve complaints have been implemented, as per Section 20 of the Standard.
6. Arrangements are in place, as per Part 6 of the Standard, to:
 - a. keep records demonstrating compliance with the Standard for a minimum of two years.
 - b. maintain the privacy and integrity of records.
 - c. securely destroy records when no longer required.

CUSTOMER INFORMATION AND NOTIFICATIONS

7. Information about the Sender ID Register is, or will be, communicated in the following ways, as per Sections 9 and 10 and Schedule 1 of the Standard:
 - a. published on your website.
 - b. communicated in writing to existing customers before 1 July 2026.
 - c. communicated in writing to new and existing customers when they request a new sender ID.
8. Public-facing communications do not inaccurately describe the matters set out at Sections 14 and 15 of the Standard.
9. If you are a carriage service provider who supplies mobile services to members of the public, communication has, or will be, provided to message recipients as per Part 7 of the Standard.

REGISTERING AND VERIFYING SENDER IDs

10. A valid use case verification is completed **before** submitting each sender ID registration application to the ACMA for an ABN entity, as per Section 11 of the Standard.
11. From 1 July 2026, the following is confirmed before enabling a customer's account to send sender ID messages, as per Section 16 of the Standard:
 - a. **Registration status:** a sender ID is registered on the SMS Sender ID Register
 - b. **Customer authorisation:** the person requesting to enable the account is authorised by the entity to which the sender ID is registered
 - c. **Telco authorisation:** the telco is authorised via the SMS Sender ID Register to send messages for that sender ID.

OFFICIAL

REGISTERING SENDER IDs ON BEHALF OF INTERNATIONAL OR EMSP PARTNERS

12. If you deal with international telcos who send sender ID messages for ABN entities, you have entered into written contractual arrangements with those telcos (international partners) to register sender identifications on their behalf, as per subsection 13(1) to (4) of the Standard.
13. If you have made arrangements with an Australian EMSP (an EMSP partner) to fulfill some or all of its obligations under the Standard, you fulfil these obligation as per subsection 13(5) of the Standard.
-

DISRUPTION AND SCAM IDENTIFICATION

14. Messages not meeting confirmation requirements (see item 11 above) will be disrupted as per Section 16 of the Standard. In particular, if the sender ID is not registered it will be over-stamped by a new sender ID of "Unverified".
15. When a scam communication is identified, the ACMA will be notified in writing within two business days, as per Section 21 of the Standard.
-

SECURITY AND PRIVACY

16. All reasonable steps have been and will be taken to ensure IT systems and processes are secure: in particular, systems for sending sender ID messages and for interacting with the Register, as per Part 25 of the Standard.
17. The ACMA will be notified in writing as soon as practicable upon the telco becoming aware of a breach or suspected breach of security.
18. If the telco is NOT already subject to the *Privacy Act 1988*, it has a documented privacy policy, trains staff on privacy requirements and destroys personal information securely when no longer needed. It does not disclose personal information to a third party except:
- as required to manage complaints
 - with the express consent of the person
 - where required/authorised by Australian law or court order.
-

REPORTING AND RECORDS

19. Reports are sent to the ACMA within 20 business days after the end of each quarter, as per Section 22 of the Standard.
20. Compliance records are kept and made available to the ACMA within five business days of a written request, as per Sections 23 and 24 of the Standard