Australian Government | acma Australian Communications and Media Authority

SMS sender ID register

Consultation on a draft industry standard and proposed register operation

MARCH 2025

Canberra
Level 3
40 Cameron Avenue
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 32
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700
F +61 2 9334 7799

Contents

Contents (Continued)

Glossary

ABN (Australian Business Number)
An entity's unique 11-digit number issued by and shown in the Australian Business Register.

ABR (Australian Business Register)
The register established under section 24 of the *A New Tax System (Australian Business Number) Act 1999*.

ACMA Assist
An online portal accessible via the ACMA's website at acma.gov.au through which the register can be accessed by entities approved under section 484F of the *Telecommunications Act 1997*.

ACN (Australian Company Number)
The unique 9-digit number given by the Australian Securities and Investment Commission to a company on registration (see sections 118 and 601BD of the *Corporations Act 2001*).

API
A set of rules or protocols that enables software applications to communicate with each other to exchange data, features and functionality.

Authorised representative (AR)
A person who has been authorised by the business administrator of an entity to access the register, and register or revoke sender IDs for that entity, but who is not authorised to grant permission to other people to access the register.

Business administrator (BA)
For an entity, a BA is:

- a person who is an authorised contact listed on the Australian Business Register (the initial business administrator), or
- a person who is granted permission to be a business administrator by the initial business administrator on behalf of the entity, and
- who is authorised to:
    - grant a person permission to be an authorised representative or a business administrator, and
    - access the register and register or revoke the registration of sender IDs for the entity.

Customer relationship management (CRM) platforms
Services designed to help businesses manage relationships with customers.

Electronic messaging service provider (EMSP)
Under section 108A of the Telecommunications Act, non-telcos that initiate SMS/MMS sender ID messages for an entity, for example, providers of software as a service and customer relationship management platforms.

Entity
An entity referred to in subsection 484F(2) of the Telecommunications Act that uses or proposes to use sender ID messages.

Originating telco
A telco that agrees to send sender ID messages on behalf of:

- customers (entities that initiate messages)
- EMSPs.

Over-stamp
Where the sender ID in an SMS/MMS message is replaced by a participating telecommunications provider with the words ‘Likely SCAM’.

Reducing Scams Code
Industry Code C661:2022 Reducing Scam Calls and Scam SMs.

Register
The SMS sender ID register.

Sender ID message
An SMS/MMS message that includes a sender ID and is sent to a mobile number issued in Australia.

Software as a service (SaaS)
A cloud-based software delivery model where users can access applications over the internet on a subscription basis.

Sender ID
Under section 484C of the Telecommunications Act, a sender ID is an alphanumeric sender ID/message header that appears at the top of SMS/MMS messages.

SMS aggregator
A carriage service intermediary that acts as an intermediary to facilitate entities sending and receiving bulk SMS/MMS messages through a single point of access.

Telcos
Carriers or carriage service providers (including SMS aggregators).

Terminating telco
A carrier that is responsible for delivering sender ID messages to message recipients who are connected to a public mobile telecommunications service owned or controlled by the carrier.

Traceback
The process of tracing the origin of a sender ID message back to the originating telco. For example, a terminating telco contacts the previous telco from which they received the message, and that telco then contacts the previous telco and so on until the originating telco is identified.

Transiting telco
A telco that connects with other telcos to transit sender ID messages between 2 telcos over a telecommunications network.

Valid use case
Evidence that demonstrates a sender ID is directly associated with the entity (the entity has legitimate reason to use the sender ID).

Overview

Short Message Service (SMS) − and Multi-Media Service (MMS) − are key communication channels used by scammers to reach Australians. In 2024, 77,365 SMS scams were reported to Scamwatch, with reported losses of over $14 million.[1] SMS scams accounted for 31% of all reported scams across all communication channels. The Australian Taxation Office reports that SMS is one of the primary channels used by scammers when targeting the community, accounting for 13.1% of impersonation scams reported from July 2024 to January 2025.[2]

Many SMS scams include some form of impersonation, where bad actors use sophisticated tactics to convince their victims they are from a legitimate entity. One common tactic is to send SMS messages with fake sender IDs (shortened brand or agency names in message headers that appear at the top of messages) to imitate well-known brands and government agencies.

To prevent these types of SMS scams, the government announced on 23 April 2023 that as part of its Fighting Scams initiative, the ACMA will implement an SMS sender ID register.

On 4 February 2025, the Minister for Communications directed the ACMA to determine a standard under the *Telecommunications Act 1997*. The standard will set out rules for the telecommunications industry to give effect to mandatory registration. The direction requires the ACMA to determine a standard by no later than 30 June 2025, and for the standard to commence in full by no later than 15 December 2025.

In brief, the way the register will work is sender IDs used by entities to send SMS/MMS messages to consumers have to be registered. If messages are sent with unregistered sender IDs, the sender ID for those messages will be replaced with the words ‘Likely SCAM’.

Registration protects against bad actors using sender IDs to impersonate legitimate entities, and protects consumers from receiving these types of scams, establishing a safe and trusted communications channel for the Australian community.

We have drafted the Telecommunications (SMS Sender ID Register) Industry Standard 2025 to enable the following objectives:

- disrupt messages with sender IDs that have not been registered
- protect end users against messages using spoofed (impersonated) sender IDs
- build public confidence in registered sender IDs
- promote consistency and accountability of actions taken by telcos for messages sent using registered and unregistered sender IDs.

The SMS and MMS ecosystem is complex and global. In this paper, we explore how we will implement a register that balances the needs of entities using sender IDs to communicate with consumers, with the requirement to protect consumers from scams.

[1] Australian Competition and Consumer Commission, ‘Scam Statistics’, Scamwatch (2024) https://www.scamwatch.gov.au/research-and-resources/scam-statistics
[2] Australian Taxation Office, Scam Channel Data, https://www.ato.gov.au/online-services/scams-cyber-safety-and-identity-protection/scam-data

Our proposed approach to the operation of the register is set out in this consultation paper, including a proposed solution overview for the register in Appendix A and registration instructions for telcos in Appendix B. The draft standard is also available alongside this paper on the ACMA website.

Issues for comment

We are seeking views from stakeholders, particularly from the telecommunications industry and businesses, agencies, and organisations that communicate with consumers via SMS/MMS (referred to as 'entities' in this paper), to help inform the design, implementation and operation of the register.

Views on how the register will deal with international entities and telcos, the types of sender IDs that can be registered, what constitutes a valid use case for sender IDs, the telco-led registration process and proposed methods of disruption are particularly welcome.

The paper poses specific questions (listed through the paper and consolidated at the end), however, we welcome feedback on any of the issues covered in the paper and the draft standard, including the proposed definitions.

We invite submissions from interested stakeholders by **Monday 28 April 2025**.

Background

Telecommunications scams have been targeting Australians on an industrial scale, with increasing sophistication and significant impacts. In addition to financial losses, scams can lead to reduced consumer trust and confidence and can have negative reputational and other non-financial impacts for businesses. For scam victims, the impact of falling for a scam can be devastating and life changing.

About sender IDs and their role in scams

What is a sender ID?

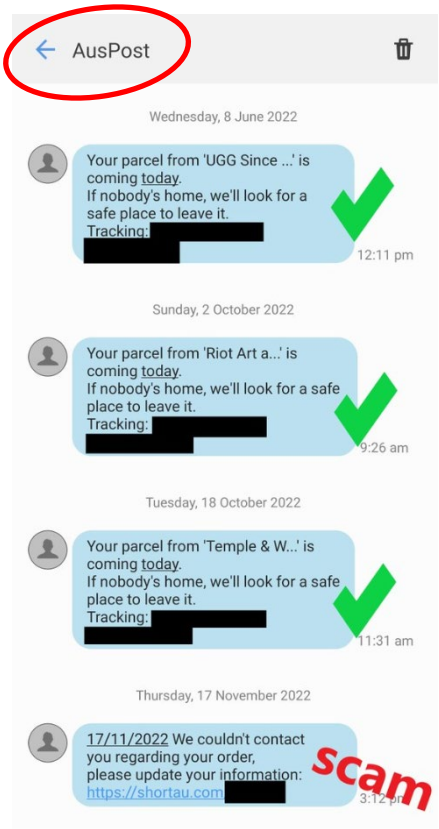
All SMS received by consumers show a sender ID at the top of the SMS – a message header – that identifies the sender of the message.

For the purpose of the register, a sender ID is an alphanumeric sender ID (for example, the shortened name of a brand or agency, such as ‘NAB’, ‘ATO’ or ‘CBA’).

Alphanumeric sender IDs are used by many well-known Australia brands and government agencies so consumers can easily identify the sender of the SMS.

Impersonating the sender IDs of well-known entities, such as banks or government services, is a key technique used by scammers to gain consumer trust, as the scam messages sent from impersonated sender IDs display in the same message thread as legitimate messages from the impersonated entity on consumer devices, as outlined in Figure 1.

Figure 1: Message thread for the sender ID ‘AusPost’ showing scam SMS in the same message thread as legitimate SMS from Australia Post



Message recipients are prompted to click on a link or call a number included in the body of the scam message. Scammers attempt to create a sense of urgency in the messages for people to respond to, for example, by claiming a bill or toll is overdue, a delivery needs to be redirected, or reward points are about to expire. This technique is used to trick message recipients to steal their money or personal information.

Impersonation of sender IDs is also harmful to entities as:

- people may stop trusting legitimate messages from entities, and/or form a negative view of the entity that the message falsely claims to come from
- recipients that have fallen victim to an impersonation scam may expect the entity that is being impersonated to reimburse them for any money they've lost or take other action to resolve the problem.

At an aggregated level, this type of scammer activity serves to decrease confidence in communications and telecommunications networks, with associated impacts from screening and avoidance behaviours.

Scope

The register only applies to alphanumeric sender IDs used to send SMS/MMS messages to Australian mobile numbers. The register ***does not*** apply:

- if the message header is a phone number[3]
- to sender ID messages sent from Australian entities to international mobile numbers
- to sender ID messages sent to international mobile numbers roaming in Australia.

Legislative arrangements and pilot

The government announced in April 2023 that the ACMA would implement an Australian register.

The *Telecommunications Amendment (SMS Sender ID Register) Act 2024*, amending the Telecommunications Act, was subsequently developed to provide the ACMA powers to establish and maintain the register.[4]

The ACMA launched a voluntary pilot register in December 2023 to provide some early protections to consumers, until legislation came into effect. The pilot has been effective as a targeted, interim measure, but is subject to limitations that make it unsuitable as a broader solution. Lessons from, and the limitations of, the pilot have informed development of the operation of the proposed register discussed in this paper.

Part 24B of the Telecommunications Act came into effect on 6 March 2025. The Minister for Communications has directed the ACMA to determine a standard under subsection 125AA(1) of the Telecommunications Act by no later than 30 June 2025.[5] The standard will set out rules for the telecommunications industry to operationalise the register. The standard, and therefore the register, must commence in full by no later than 15 December 2025.

[3] The Industry Code C661:2022 Reducing Scam Calls and Scam SMs includes obligations on all originating telcos to prevent carriage of SMs using telephone numbers where the sender does not hold the rights of use to the number.
[4] Telecommunications Amendment (SMS Sender ID Register) Act 2024.
[5] Federal Register of Legislation - Telecommunications (SMS Sender ID Register Industry Standard) Direction 2025.

We will use information obtained through this consultation process to further progress the standard and develop determinations that will relate to:

- applications to participate in the register and register sender IDs
- administration of the register
- access to the register.

We anticipate consulting on these determinations in coming months.

Objectives of the register

The register will disrupt scams that impersonate sender IDs, protect entities subject to SMS impersonation scams (including backs, retailers, road-toll companies and government agencies) and establish a safe and trusted communications channel for the Australian community.

These objectives will be achieved by:

- only allowing legitimate entities and their authorised contacts to participate in the register and register sender IDs
- requiring registration of all sender IDs that are used to send messages to Australian mobiles
- requiring telcos to only send, transit and terminate messages with registered sender IDs
- requiring telcos to over-stamp messages from unregistered sender IDs with 'Likely SCAM'.

The register is part of a suite of Australian Government initiatives to combat scams and protect Australians from financial harm, including the standing up of the National Anti-Scams Centre and introduction of the Scams Prevention Framework (SPF).[6]

These broader scam reduction activities, including telco obligations for SMS scams generally, will be covered by the SPF, which is expected to come into effect in early 2026.[7]

The government has indicated that the ACMA will be designated as the sectoral regulator for the telecommunications sector under the SPF, and will be involved in developing a new code that would replace the existing Industry Code C661:2022 Reducing Scam Calls and Scam SMs (Reducing Scams Code) registered by the ACMA under Part 6 of the Telecommunications Act.

[6] Scams Prevention Framework – Protecting Australians from scams | Treasury.gov.au.
[7] Scams Prevention Framework Bill 2025 – Parliament of Australia.

Model

Following consultation and an impact analysis, the government announced on 3 December 2024 that a mandatory registration model will be implemented in Australia.[8]

Under the ACMA's proposed mandatory registration model:

- Telcos must be approved by the ACMA to participate in the register. Non-participating telcos will not be permitted to send, transit, or terminate sender ID messages, so sender ID messages from non-participating telcos will effectively be **blocked** (the intended recipient will not receive the message).
- Originating and terminating telcos that have been approved to participate will be required to **over-stamp** unregistered sender IDs. This means unregistered sender IDs will be removed from messages and replaced with a new sender ID, such as 'Likely SCAM' (the recipient will receive the message, but the message header will be 'Likely SCAM', to alert the recipient that the message may be a scam).

Figure 2 below sets out an overview of the proposed model.

We are proposing to take a graduated approach to disrupting unregistered sender IDs (as discussed in the 'Disruption method' section below). Unregistered sender IDs will initially be over-stamped. After 12 months, we propose to assess the effectiveness of over-stamping. Depending on the outcome of the assessment, we may consider implementing another disruption method, for example, blocking all messages with unregistered sender IDs.

The register rules do not require an assessment of whether sender ID messages are scams. This means that messages from non-participating telcos or with unregistered sender IDs will be disrupted regardless of whether they are scams. Entities must register sender IDs to avoid disruption of their sender ID messages.

The register does not affect existing telco obligations under the Reducing Scams Code to monitor, identify and block scams, or any future obligations under the Scams Prevention Framework. Under the Reducing Scams Code, telcos have obligations to conduct 'Know Your Customer' checks for all originating traffic, including for SMS/MMS, and to monitor and take action against scam traffic. The register complements these arrangements with robust Know Your Customer measures.

[8] https://minister.infrastructure.gov.au/rowland/media-release/better-protections-australians-sms-scams

Figure 2: Overview of the operation of the SMS sender ID register

Entity registration

The Telecommunications Act sets out certain requirements for participating in the register (section 484F) and registering sender IDs (section 484G). This section overviews the proposed process for approval of entities to use the register. The next section deals with approval of specific sender IDs by approved entities.

Participating entities

The Telecommunications Act requires entities that wish to participate in the register to apply to the ACMA for approval.[9]

Only the following types of entities may participate in the register:

(a) an individual

(b) a body corporate

(c) a corporation sole

(d) a body politic

(e) a government entity (within the meaning of the *A New Tax System (Australian Business Number) Act 1999*)

(f) a partnership

(g) any other unincorporated association or body of persons

(h) a trust

(i) a superannuation fund (within the meaning of the *Superannuation Industry (Supervision) Act 1993*).

An application to participate in the register must:

- be made using a form published by the ACMA on its website
- contain the information required by the form
- be accompanied by any applicable charge
- comply with any other requirements determined by the ACMA.

The ACMA may make a determination under subsection 484L(1) of the Telecommunications Act that sets out the criteria that must be met for an entity to be approved to participate in the register.

[9] Subsection 484F(1)

Participant registration requirements

To minimise the possibility of 'bad actors' accessing the register, our proposed registration approval process is designed to meet the following requirements:

- the person who applies on behalf of an entity is a real person
- the person is who they say they are (that is, not someone who has stolen an ID and is impersonating that person)
- the entity the person represents is legitimate and is covered by subsection 484F(2) of the Telecommunications Act
- the person who applies is an authorised contact for that entity.

Once the ACMA has approved an entity to participate, the process for adding additional register users for that entity will confirm:

- the person adding a new register user is a real person and a business administrator for the entity
- the person being added as a new user is a real person.

The ACMA may also include additional criteria in a determination, for example, that a business administrator can only add entity employees or agents to the register.

Australian entities

To meet these requirements, we propose to implement the following approval process for Australian entities:

- Entities can access the register through the ACMA Assist online portal.
- A person listed as an authorised contact for an entity on the Australian Business Register (ABR) will set up a register account through the ACMA Assist online portal. ACMA Assist currently requires users to verify their identity using Australia Post's Digital ID service or the government's myID app. Both methods require an Australian-issued identity document such as a passport, driver's licence, birth or citizenship certificate. Subsequent access to ACMA Assist (and therefore the register) requires multi-factor authentication.
- The person making the application will be cross-referenced against the ABR to verify they are an authorised contact for the entity. People listed on the ABR's authorised contact list automatically become business administrators for that entity and can access the register (after they have successfully completed the ACMA Assist identity verification requirements). Business administrators have full access to their entity's register account and can add other business administrators or authorised representatives for that entity.
- Business names associated with an entity can be included in a centralised account in the register for the entity.
- The entity will be cross-referenced against the ABR to verify it is legitimate.
- Business administrators and authorised representatives will be linked to a specific entity's account and will only be able to view or make changes to information for that entity. The name and contact details of all business administrators and authorised representatives will be recorded by the ICT system for the register.
- Before accessing the register, users will be required to agree to the register's terms of use.

Question 1
Are there any other requirements that the participant application process should include?

Question 2
Excluding overseas entities, will the requirement to cross-reference entities against the ABR prevent or impede any sector of the Australian market that uses sender ID messages from participating in the register?

Question 3
Will requiring entity accounts to be set up/approved by entity representatives listed on the ABR be a barrier to participation? If so, how can this be overcome without compromising the registration requirements?

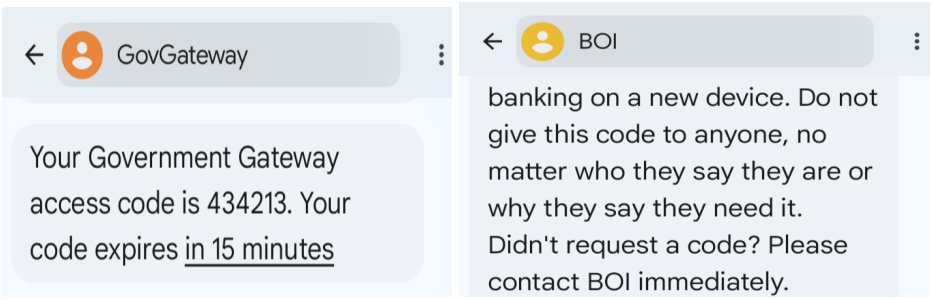
International entities

International entities that send messages with sender IDs to Australian mobile numbers will need to have a registered Australian business to participate in the register under the proposed model (see also 'International telco' section below).[10]

There are significantly higher risks if international entities are allowed to participate in the register without adequate safeguards. For example, the ACMA would be unable to readily verify the legitimacy of international entity documents (such as company registrations).

We understand, however, that there are currently international entities without a registered business in Australia that may send sender ID messages to Australians, for example, overseas government agencies and businesses, as outlined in Figure 3.

Figure 3: Example of international messages from the UK government's service portal (GovGateway) and Bank of Ireland (BOI)



International models

Singapore operates a mandatory sender ID register, which means that all entities wishing to send SMS messages to Singaporean mobile numbers using a sender ID must register those IDs.

Foreign-based businesses must obtain a local unique entity number (UEN) from the government to sign up with the sender ID register and protect the sender IDs they wish to use to send messages to Singapore mobile users. Foreign-based businesses can obtain a

[10] International entities that contact travellers who are using mobile roaming while visiting Australia (that is, are not using Australian mobile numbers) are out of scope for the register.

UEN by registering with the Accounting and Corporate Regulatory Authority in Singapore. A foreign business can either register as local subsidiary or register as a foreign branch office.

In the United Kingdom, a voluntary sender ID register is operated by the industry body, Mobile Ecosystem Forum. Organisations that want to register sender IDs are required to provide a letter of authorisation to the Mobile Ecosystem Forum and/or their preferred SMS aggregator. As the UK register is voluntary and administered by industry, there are no legislative requirements to participate.

Question 4
Should the register only allow entities with an Australian presence (that is, an ACN and/or ABN) to participate in the register? If yes, what would be the likely impact of disrupting international messages that use sender IDs?

Question 5
Do you propose any alternative approaches to allow international entities to participate, which still meet the register objectives and do not compromise the effectiveness/security of the register? For example:

- Could there be arrangements that allow an Australian telco or entity to act as a proxy for an international entity for the purposes of the register?
- Should these arrangements be limited to certain types of international entities? If so, which types?
- How would any such arrangements be secure and prevent bad actors from registering sender IDs associated with scam communications?
- Where should compliance obligations rest, given the ACMA does not have jurisdiction over foreign telcos or entities?

Registration process – telco-initiated

We have included obligations in the draft standard for originating telcos to initiate registration on behalf of entities. An application will only be accepted by the ACMA if:

- it is initiated by an originating telco that has been approved by the ACMA to participate in the register
- the entity that uses the sender ID is successfully verified by the ACMA (in accordance with the ‘Participating entities’ section above)
- the entity approves the registration.

Transitional obligations

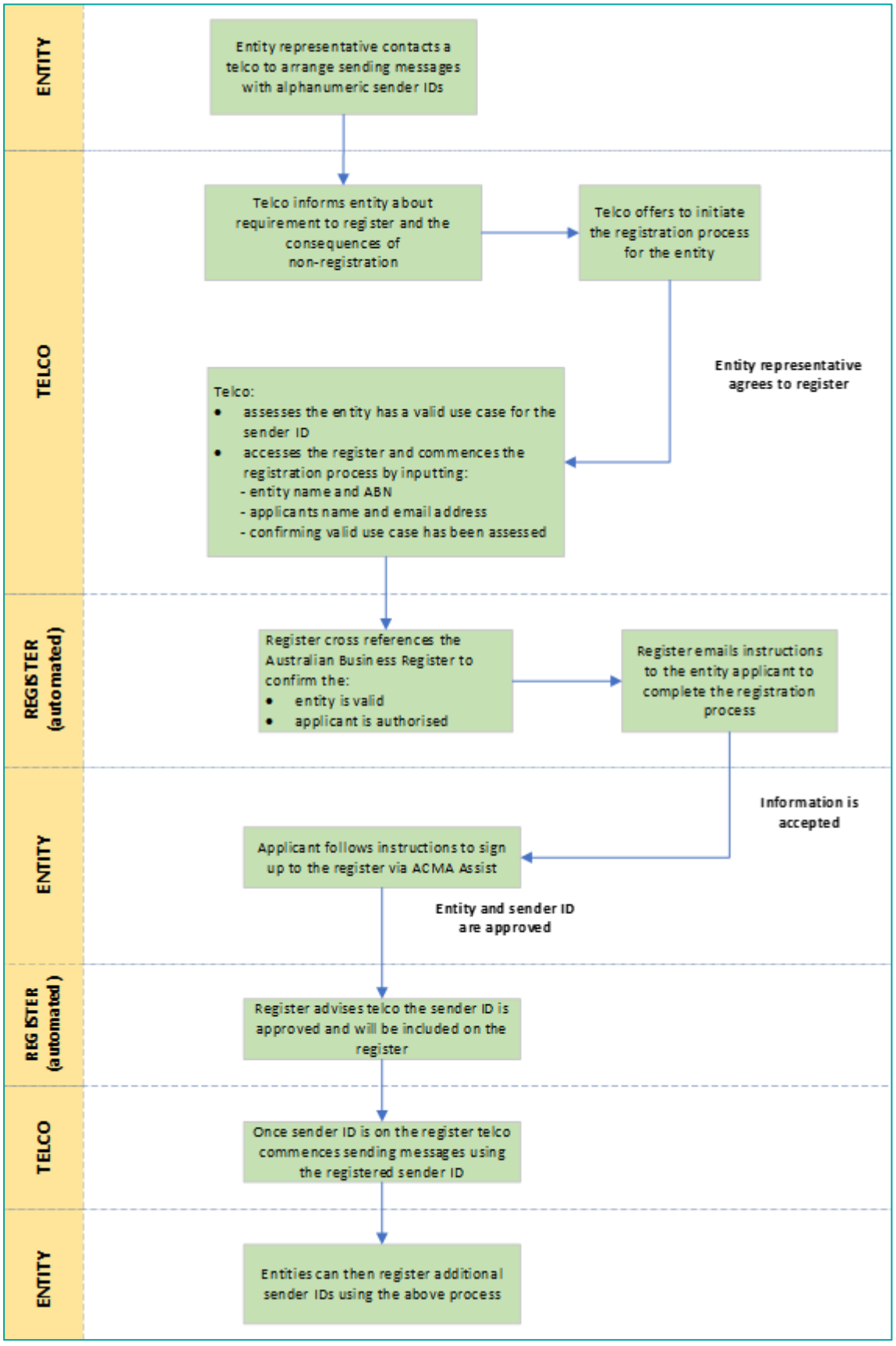
Before the register starts, originating telcos would be required to contact customers (entities) with which they have existing arrangements to send sender ID messages, and:

- provide information about the register and the registration process
- advise that messages sent with unregistered sender IDs after 15 December 2025 will be disrupted
- offer to initiate registration on behalf of the customer.

If the customer agrees to register, the originating telco must initiate the registration process on behalf of the customer. This will then trigger communication to the customer from the ACMA that clearly explains what the entity needs to do to finalise registration – see Figure 4

for an example of the telco-initiated registration process and ‘Registration instructions for originating telcos’ at Appendix B.

Figure 4: Example of telco-initiated registration process



Ongoing obligations

There will be ongoing obligations for originating telcos to provide information about the register and offer to initiate registration when:

- a new customer asks the telco to send messages with sender IDs
- an existing customer asks the telco to send messages using a new sender ID.

The originating telco would **not** need to confirm the identity of the person making the request, or if the entity is legitimate before initiating a registration application, as identities are confirmed via ACMA Assist before accepting the registration application.

If an entity does not confirm a telco-initiated application, or fails the verification process in ACMA Assist, registration would not proceed.

Once a sender ID is registered, entities can use the register to authorise other originating telcos to send messages using that sender ID. Initiating registration through a particular telco does not mean the entity can only use that telco. Entities can also use the register to revoke authorisations for telcos to send messages for registered sender IDs.

This approach recognises that sending messages with sender IDs is a long-established practice in Australia, with existing processes and commercial arrangements in place between telcos and entities. Leveraging these arrangements is likely to result in efficiencies and less duplication than other potential arrangements.

The proposed telco-initiated registration process is included in the draft standard, which is available alongside this paper, the proposed solution overview is described at Appendix A and the telco registration instructions are in Appendix B.

The advantages of a telco-initiated registration process include:

- The registration process would be an extension of current practice, where entities contact originating telcos (or electronic messaging service providers (EMSPs), such as software-as-a-service (SaaS) providers or customer relationship management (CRM) platforms) to initiate messaging. Originating telcos are already required to establish valid use cases to comply with the Reducing Scams Code.
- It allows for originating telcos to verify sender IDs on behalf of others, such as EMSPs. It also more readily allows for potential future expansion to include Rich Communication Services (RCS) messaging, as the RCS verification authority standard follows a telco-initiated registration approach.[11]
- Because originating telcos know which entities are using sender IDs, they are best placed to inform them of the requirement to register.

A risk of telco-initiated registration is that it relies on originating telcos complying with the rules. Our experience enforcing the Reducing Scams Code indicates not all telcos comply with their obligations.[12] The ACMA will actively enforce the standard and act against telcos that do not comply. Failing to comply with an industry standard is a contravention of section 128 of the Telecommunications Act. If contraventions are established, the ACMA has the

[11] Introduction: 927_GSMA-RCS-Verified-Sender-report-v5.pdf, Specification: NG.131 RCS Verification Authority API v0.1 (Current).
[12] For example: Five telcos breached for allowing SMS scams | ACMA.

power to take enforcement action, including issuing a formal warning, giving an infringement notice, entering into an enforceable undertaking and commencing civil proceedings.[13]

The government's proposed carriage service provider registration scheme, when enacted, would also provide a fundamental enabler to effective compliance and enforcement.[14]

Registration process – entity-initiated

Once the register begins, entities could also apply directly to the ACMA to register, rather than going through originating telcos. This process will largely be similar to the telco-initiated process, but the ACMA, not the telco, will establish whether an entity has a valid use case before accepting registration of a sender ID.

Question 6
Do you support telco-initiated registration? Please explain your reasons.

If yes, is the ACMA's proposed approach (where originating telcos initiate registration but entities must confirm) suitable/workable?

Question 7
If you are an originating telco, do the instructions at Appendix B raise any issues for you?

Revoking participant approval

The ACMA may, in writing, revoke approval of an entity if the ACMA is satisfied under subsection 484F(7) of the Telecommunications Act that it would be appropriate in all the circumstances to do so. The explanatory memorandum associated with the amendments to the Telecommunications Act includes the following examples:

- if it becomes apparent that an applicant has currently or previously submitted information that is untruthful in an approval application
- if the applicant is charged with offences connected to scam activity
- if it becomes apparent that an applicant has been involved in scam activity or has previously been connected to a business or entity that has previously been involved in scam activity.

Question 8
What types of circumstances or behaviour do you consider should cause the ACMA to consider revoking an entity's approval and how would the ACMA become aware of it?

[13] https://www.acma.gov.au/compliance-and-enforcement-policy.
[14] Albanese Government takes strong action to protect telco consumers | Ministers for the Department of Infrastructure.

Sender ID registration

Under subsection 484G(1) of the Telecommunications Act, only an entity that has been approved to participate in the register can apply to register sender IDs.

Registration criteria – applicant's identity

We propose to implement a sender ID approval process that confirms:

- the person registering the sender ID has the authority to register sender IDs on behalf of the entity. This will initially be done via the ABR and then via ACMA Assist.
- the person is who they say they are (that is, not someone impersonating a real person who is an authorised representative of the entity). This will be done via ACMA Assist.
- the entity has a 'valid use case' for the sender ID. This means the entity is able to prove a sender ID is directly associated with the entity (see 'Valid use case' section below).

Registration criteria – sender IDs

We propose that a sender ID must meet certain criteria to be registered. These criteria will be included in a determination made by the ACMA under subsection 484L(1) of the Telecommunications Act. Sender IDs that do not met these criteria will not be registered.

We propose that to be registered, sender IDs must:

- be at least 3 and no more than 11 characters long
- with limited exceptions (see below), include letters, or a combination of letters (A-Z), numbers (0–9) and symbols, but cannot consist only of numbers. Sender IDs will be case-insensitive (for example, 'ABC' is treated the same as 'abc')
- start with a letter, with limited exceptions (see below)
- not contain non-Latin characters
- only contain the following symbols: + - _ &
- not contain a space or underscore at the beginning or end.

We note that while the Telecommunications Act allows for sender IDs to consist solely of symbols, in practice, we expect there would be very limited circumstances, if any, where symbol-only sender IDs are registered. This is because we propose:

- entities must establish a valid use case for a sender ID before it can be registered
- only 4 symbols will be permitted in sender IDs: + - _ &

We propose that the same sender ID can be registered by multiple entities, provided each entity has a valid use case. For example, all entities that have 'ACMA' as their acronym could register 'ACMA' as their sender ID.

Additional criteria

We are considering whether to limit the number of sender IDs an entity can register. Limiting the number of sender IDs that can be registered (and therefore used) by each entity would help consumers identify the sender of a message. For example, if an entity only used one sender ID, there would be a clear association between that sender ID and the entity. All the messages would appear in the same message thread, further reinforcing that association.

If an entity only uses one or 2 sender IDs, it can provide clear guidance to its customers about which messages to trust, for example, the ACMA will only send you messages using the 'ACMA' sender ID.

Limiting the number of sender IDs per entity may also help consolidate and reduce data recording and reporting requirements associated with the register.

To prevent the registration of spoofed (impersonated) sender IDs, as required by subsection 484G(5) of the Telecommunications Act, we propose that a sender ID must be directly associated with the entity's name or one of their brand names (see 'Valid use case' section below).

Question 9
Should any additional symbols (e.g. '!' '#' '%' '?') be permitted for sender IDs?

Question 10
Should there be any other format limitations for sender IDs?

Question 11
Should the register be case sensitive (that is, lowercase and uppercase letters are required to match exactly)?

Question 12
Should there be a limit on the number of sender IDs that can be registered by an entity? If so, what should that limit be?

Question 13
Do you agree that the same sender ID could be used by multiple entities, provided each entity can establish a valid use case? Please explain your reasons.

Valid use case

If an originating telco is initiating registration of a sender ID for an entity, the telco will be required to establish that the entity has a valid use case for that sender ID. A valid use case means an entity can prove a sender ID is directly associated with the entity.

We propose that originating telcos would be required to establish that an entity has a valid use case by:

- confirming that the sender ID is directly associated with the entity's name, for example, by matching the sender ID to entity's registered name on the ABR, or
- requiring an entity to submit evidence proving that the sender ID is directly associated with one of the entity's brand names, for example, a letter or document that proves the brand name (and therefore the sender ID) is associated with that entity.

For example, if the ACMA attempted to register 'ACMA-alert', the sender ID would be accepted. However, if the ACMA attempted to register 'Telco alert', it would not be accepted unless the ACMA could provide evidence that 'Telco alert' is an ACMA brand name.

This means that in most circumstances, the purpose of the message would have to be included in the body of the message. For example, instead of Retailer X using 'Stocktake' as a sender ID, they would have to use 'Retailer X' as the sender ID and include 'Stocktake' in the body of the message.

We appreciate that this is a change from the way some entities currently use sender IDs. However, this approach significantly simplifies and improves messaging practices for entities and delivers better outcomes for consumers.

Requiring a clear relationship between a sender ID and an entity will:

- help prevent the registration of offensive, misleading, deceptive, spoofed, or generic sender IDs
- improve consumer brand recognition and trust in entities. It is easier for consumers to recognise who messages are from, and therefore to identify any anomalies, and participation in the register will increase consumer trust.

There is no requirement to establish a valid use case for unregistered sender IDs, as unregistered sender IDs will be over-stamped (see 'Disruption method for unregistered sender IDs' below).

Question 14
Is the ACMA's proposal to require sender IDs to be directly associated with an entity's name or a brand name workable? Do you agree this approach helps prevent the registration of spoofed/misleading/deceptive/generic sender IDs? Please explain the reasons for your response.

Question 15
What alternative measures could be taken to confirm an entity has a valid use case for a sender ID?

Removing sender IDs from the register

We may remove a registered sender ID from the register (under section 484H of the Telecommunications Act) if we are satisfied that it is offensive, misleading, deceptive, spoofed, or if it is appropriate to do so; for example, the sender ID is only used by one entity and that entity has ceased trading.

Question 16
Are there other circumstances where the ACMA should remove sender IDs from the register?

Sending messages

Australian telcos

We propose that all Australian telcos that send, transit and/or terminate messages with sender IDs will be required to apply to the ACMA for approval to participate in the register under section 484F of the Telecommunications Act. The telco application process will include verification of the telco and the identity of the telco's authorised contact/s.

Only approved telcos (participating telcos) will be permitted to:

- send, transit and terminate messages with sender IDs
- initiate registration on behalf of entities.

Participating telcos will not be permitted to send messages with sender IDs to, or transit or terminate messages from, non-participating telcos. This means that messages that come from non-participating telcos will effectively be blocked.

In January 2025, the government announced it will establish a carriage service provider registration scheme to increase visibility of providers in the market.[15] To reduce impost, telco approval to participate in the register could potentially be linked to this scheme once it is operating.

Our proposed approach is similar to the Singapore Sender ID Registry, in that only 'Participating Aggregators' (PAs) that are licensed can be involved in the registry.[16]

Overview of proposed telco rules

The proposed rules that will apply to participating originating, transiting and terminating telcos are set out in the draft standard and outlined below. These obligations are based on the functions of telcos in the supply chain. This means that a telco could be an originating telco in some circumstances, and a transiting or terminating telco in others. All participating telcos will be required to implement policies and procedures to comply with the standard.

To provide telcos an opportunity to update their systems when new sender IDs are added to the register, we propose that updates occur within a 24- (or 48-) hour period from 11.59 pm on the day on which a sender ID is registered. This would ensure telcos have up-to-date register data and reasonable discretion about exactly when to update within the given period.

Originating telcos

In the proposed model, 'originating' telcos are telcos (including SMS aggregators) that send sender ID messages for:

- entities (commonly referred to by telcos as the A-Party)
- EMSPs – non-CSPs that initiate SMS/MMS sender ID messages for the entity (A-Party), for example, providers of SaaS or CRM platforms
- potentially international telcos/entities (if international entities are permitted to participate – see 'International entities' section above and 'International telcos' section below).

[15] Albanese Government takes strong action to protect telco consumers | Ministers for the Department of Infrastructure
[16] https://www.sgnic.sg/faq/sms-sender-id-registry

We considered placing obligations directly on EMSPs, but formed the view that telcos are better placed to participate in the register because EMSPs:

- are not currently captured by telco regulations and many are located offshore, meaning we cannot enforce compliance with register rules
- provide software over the internet for users to manage multiple services (not necessarily including or limited to communications).

We also understand that some SMS aggregators already have processes in place that are consistent with our proposed approach.

Originating telcos would be required to:

- only send messages with sender IDs if the sender ID is registered, and over-stamp unregistered sender IDs
- only send messages with registered sender IDs to other telcos participating in the register
- comply with the obligations outlined in the 'Telco initiated registration' and 'Valid use case' sections above when initiating registration of a sender ID for an entity.

Transiting telcos

In the proposed model, 'transiting' telcos are telcos that connect with other telcos to transit sender ID messages between 2 telcos over a telecommunications network.

Transiting telcos would be required to:

- only accept messages with sender IDs from other telcos participating in the register
- only send messages with sender IDs to other telcos participating in the register.

Transiting telcos are not required to check if a sender ID is registered. The draft standard includes an exemption that allows transiting telcos to forward sender ID messages (via international telcos) to Australians mobile users who are roaming overseas.

Terminating telcos

In the proposed model, 'terminating' telcos are carriers that are responsible for delivering sender ID messages to message recipients (commonly referred to by telcos as the B-Party) who are connected to a public mobile telecommunications service owned or controlled by the carrier. In this context 'terminate' means to deliver messages to message recipients.

Terminating telcos would be required to:

- only accept messages with sender IDs from other telcos participating in the register
- terminate any messages with registered sender IDs
- over-stamp messages with unregistered sender IDs.

Requiring terminating telcos to over-stamp unregistered sender IDs is an additional precaution to guard against an originating or transiting telco not having followed the correct procedure.

Non-participating telcos

The draft standard includes rules that prohibit non-participating telcos from:

- sending, transiting or terminating sender ID messages
- misrepresenting themselves as a participating telco.

Question 17
Is within 24- (or 48-) hours after 11.59 pm on the day a sender ID is registered an appropriate amount of time for telcos to update their systems with sender ID data? Would another period be preferrable? Please provide details to support your response.

Question 18
Do you have any comments or concerns about how originating, transiting, and terminating telcos are defined?

Question 19
Are the proposed obligations for originating, transiting, and terminating telcos appropriate? If not, what would prevent each type of telco from meeting the proposed requirements? What exceptions should be included?

Question 20
The proposed model requires messages with sender IDs to only be sent, transited or terminated by telcos participating in the register. Does this model pose any issues and, if so, what, for:

- telcos
- EMSPs
- entities?

Question 21
Is the proposal for terminating telcos to over-stamp unregistered sender IDs required and/or supported? We are interested in views from across the sector, including those of terminating telcos.

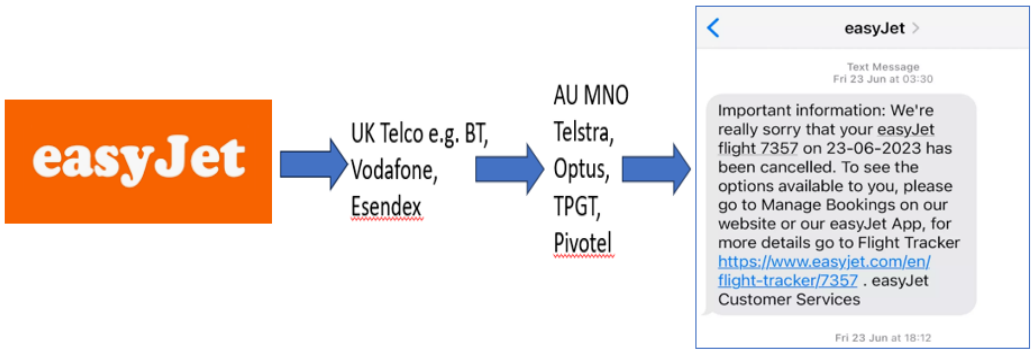
Question 22
Does the solution overview proposed at Appendix A raise any issues for telcos?

International telcos

To ensure the effectiveness of the register, and as the ACMA is only able to enforce rules against Australian telcos, we propose that only telcos with a registered Australian business presence be allowed to participate in the register.

We acknowledge, however, that if international entities were permitted to participate in the register (as discussed in the 'International entity' section above), international telcos could be used to send/transit those messages, as illustrated in Figure 5.

Figure 5: Example of British airline easyJet using a UK telco to send a message using a sender ID (easyJet) to an Australian resident



We are seeking views on whether arrangements should be implemened to allow the receipt of sender ID messages from an international (and therefore non-participating) telco, and if so, what such arrangements could be, without compromising the security and effectiveness of the register.

International examples

As previously noted, in Singapore only Participating Aggregators (PAs) that have been licensed can be involved in the Singapore Sender ID Registry. If a telco or aggregator does not wish to be licensed or participate in the registry, it must reroute SMS traffic through other PAs to ensure that the protection of the sender ID works correctly.[17]

In Finland, SMS traffic using registered sender IDs must be routed via the application interfaces provided by Finnish telecommunications companies. SMS traffic using registered SMS sender IDs from international gateways and APIs must be blocked.[18]

Question 23

Noting that:

- the ACMA proposes only participating telcos can receive messages with sender IDs, and
- only Australian telcos can participate in the register,

should arrangements be implemented to allow the receipt of sender ID messages from an international (and therefore non-participating) telco? For example:

- could an Australian telco who receives sender ID messages from international telcos be considered an originating telco and be required to validate the sender ID (as set out in the 'Originating telcos' section above)?
- how would such an arrangement work? Are there any alternative approaches that would meet the register objectives and would not compromise the effectiveness or security of the register?

[17] https://www.sgnic.sg/faq/sms-sender-id-registry.
[18] Protecting an SMS Sender ID.

Disruption method – unregistered sender IDs

The government has announced registration of sender IDs will be mandatory (see 'Registration model' section above). To implement this decision, we are proposing that:

- **Only participating telcos will be permitted to send, transit and terminate messages with sender IDs**. This means that messages that come from non-participating telcos will effectively be blocked.
- **Participating originating telcos will be required to over-stamp unregistered sender IDs** before sending messages to participating transiting/terminating telcos.
- **Participating terminating telcos will be required to over-stamp messages with unregistered sender IDs** before terminating messages.

We are open to considering, however, whether unregistered sender IDs should be blocked instead of over-stamped. Table 1 sets out the key limitations and benefits of each option.

Table 1: Disruption method benefits and limitations

Key benefits	Key risks
Preferred option: over-stamping – replace all unregistered sender IDs with 'Likely SCAM' before messages reach consumers	
• A sender ID of 'Likely SCAM' will alert consumers that the message may not be legitimate. • Boost consumer confidence that messages with sender IDs that haven't been replaced by 'Likely SCAM' are legitimate. • Messages from unregistered sender IDs that are not scams will still be received by consumers. They will appear in a message thread titled 'Likely SCAM'. • The Singaporean experience has shown over-stamping can provide effective disruption. A 2023 Singaporean consumer survey showed that 4 in 5 respondents agreed that the 'Likely-SCAM' label made them more cautious about whether the SMS is real or fake, and 92% would choose to delete or ignore an SMS labelled 'Likely-SCAM'.[19]	• Consumers will still receive scams. They will appear in a message thread titled 'Likely SCAM'. • Consumer confusion if messages they believe or know to be genuine have come from a 'Likely SCAM' sender ID. • Consumer fatigue if they receive many 'Likely SCAM' messages. • Communicating benefits to consumers is less simple – e.g. 'if you receive a message with a sender ID of 'Likely SCAM', you need to exercise caution because it may be a scam.'

[19] SSIR Likely-SCAM Online Study conducted by MCI in Jun 2023 with more than 1,000 Singapore residents aged 15 and above to understand public responses to the "Likely-SCAM", Singapore Police midyear scam and cybercrime statistics 2023, page 17.

Key benefits	Key risks
Alternative option: blocking − stop messages from unregistered sender IDs reaching consumers	
• Scam messages with sender IDs don't get through to consumers. • Harms from scam messages with sender IDs are reduced. • Boost consumer confidence that messages with sender IDs are legitimate. • As a result of increased consumer confidence, increase in consumer engagement with messages that use sender IDs. • Simple to communicate benefits to consumers – e.g. 'if you receive a message with a sender ID, you can be confident it is legitimate.'	• Legitimate messages are not received by consumers because the sender ID has not been registered. This could result in important or time critical messages (such as for overdue bills or medical appointments) not being received.

The ACMA proposes to review the effectiveness of the chosen disruption method after 12 months of operation. Data to inform this review will include statistics reported under the standard, broader scam report trends across government, and stakeholder feedback, including via consumer scam reports.

International examples

Singapore's SMS Sender ID Registry transitioned to a mandatory registration scheme after 12 months of operation, with all unregistered sender IDs replaced with 'Likely-SCAM'. [20]

The UK's Sender ID Protection Registry is voluntary.[21] Messages are blocked if the sender's details do not match the details registered against a registered sender ID. A block list is kept to prevent misuse of sender IDs that closely resemble registered IDs. Unregistered sender IDs are not affected.

Ireland's Sender ID Registry mandates registration of *s*ender IDs by *s*ender ID owners.[22] As at February 2025:

- SMS aggregators and mobile service providers handling bulk SMS traffic on behalf of organisations need to pre-register the SMS sender IDs used by those organisations by 25 February 2025.[23]
- For a transition period from 3 July to 2 October 2025, any unregistered SMS sender IDs or SMS messages from registered sender IDs that are sent via an unapproved route will be modified to alert end-users that the sender ID cannot be trusted and the SMS may not

[20] https://www.sgnic.sg/smsregistry/overview
[21] SMS SenderID Protection Registry - Mobile Ecosystem Forum
[22] https://www.comreg.ie/media/2024/12/ComReg-2497_Implementation-and-Communications-Plan-for-SMS-Sender-ID-Registry.pdf
[23] https://www.comreg.ie/sms-sender-id-registry-in-ireland-sms-aggregators-and-mobile-service-providers-msps-need-to-pre-register-existing-sms-sender-ids-by-25-february-2025/

be genuine. Ireland is considering the precise sender ID that will be used for modified SMS.

- From 3 October 2025, Ireland intends for any unregistered SMS sender IDs or SMS from registered sender IDs that are sent via an unapproved route to be blocked from transmission by participating SMS aggregators and mobile service providers.

Hong Kong's SMS Sender Registration Scheme is voluntary.[24] Rather than identifying or blocking unregistered sender IDs, registered senders use a '#' at the beginning of their sender ID, for example, #BUSINESS. This marks the sender ID as registered, so it is clearly labelled for consumers.

Question 24
The ACMA is proposing that only participating telcos will be permitted to send, transit and terminate messages with sender IDs, which effectively blocks messages from non-participating telcos. Should messages from non-participating telcos be over-stamped instead? Please explain your reasons.

Question 25
Given the risks and benefits of over-stamping versus blocking, do you agree with the ACMA's graduated disruption approach − to initially over-stamp unregistered sender IDs and subsequently consider blocking? Are there other disruption options or transitional arrangements that should be considered?

Question 26
If unregistered sender IDs are over-stamped rather than blocked, what term should be used − 'Likely SCAM', 'unverified', or something else?

[24] https://www.ofca.gov.hk/en/consumer_focus/guide/hot_topics/ssrs/index.html.

Complaints handling

An effective complaints-handling process for the register will assist us to identify areas for improvement, address concerns and effectively enforce compliance with the register. The process for handling complaints may depend on who the complaint is from and what the complaint is about.

Noting that:

- the Telecommunications (Consumer Complaints Handling) Industry Standard 2018 is already in force and applies to complaints that telcos receive from consumers and certain types of business (small businesses), and
- the Scams Prevention Framework currently under development will include internal and external complaints-handing obligations,

we propose to include complaint-handling obligations in the standard requiring participating telcos to implement policies and procedures to deal with, record and resolve complaints from entities (irrespective of size) relating to the telco's application of the register rules. This includes complaints about failing to provide accurate information about the register to a customer or incorrectly disrupting sender ID messages.

The proposed rules that will apply to participating originating, transiting and terminating telcos are set out in the draft standard.

We will make information about the ACMA's complaint-handling processes for the register available on our website. The ACMA will generally deal with complaints about:

- the general operation of the register/underpinning policy
- telco non-compliance with the register.

The ACMA will handle register enquiries, including support requests, and complaints during regular business hours − Monday to Friday from 9 am to 5 pm AEST, excluding public holidays.

Participating telcos will also be required to handle basic enquiries about the operation of the register.

Reporting and traceback

We require information to administer the register, monitor its effectiveness and enforce compliance.

Certain information can be obtained directly from the register, for example, the number of participating telcos, a list of registered sender IDs, which telcos are initiating sender ID registration for entities, and which telcos are authorised to send messages for each registered sender ID. However, we will require telcos to report information that the ACMA cannot source directly from the register.

While information reported by telcos may provide valuable information to support broader scam reduction activities, the proposed reporting and traceback obligations are limited to supporting the register. We note that the Reducing Scams Code already includes some reporting requirements, and broader scam-related reporting obligations (including information sharing) will be included in the Scams Prevention Framework.

We propose to require participating telcos to report to the ACMA on a quarterly basis:

- the number and type of complaints participating telcos have received from other telcos, entities and end users about the register (all telcos)
- the number of messages sent for each registered sender ID (originating telcos)
- the number of messages sent for each unregistered sender ID (originating telcos)
- the identity of non-participating telcos that have attempted to send sender ID messages (transiting and terminating telcos)
- the number of messages received from participating telcos (terminating telcos)
- the number of unregistered sender IDs that have been over-stamped by terminating telcos (terminating telcos).

We propose to require all participating telcos to:

- report any scams that they have identified for messages sent using registered sender IDs. This would include scams identified via their own scam detection processes or via complaints or reports
- traceback those messages to identify the originating telco.

These rules build on current traceback requirements in the Reducing Scams Code. The information obtained via the traceback requirements in the draft standard will enable the ACMA to promptly investigate potential non-compliance or compromise of the register and, if warranted:

- remove sender IDs used to send scams from the register
- remove non-compliant telcos from the register.

If the traceback rule in the standard comes into effect before the Reducing Scams Code is amended, the ACMA will enforce the rule in the standard. As noted in clause 1.1.5 of the code, if there is a conflict between the requirements of the code and any requirements imposed on a telco by statute, the telco will not be in breach of the code by complying with the requirements of the statute.

The proposed reporting rules are set out in the draft standard.

Question 27
Is there any other information about the register telcos should be required to report to the ACMA? Do telcos have a preference for how these reports should be provided, for example automated or API reporting?

Question 28
Are there any obstacles to originating telcos collecting data on the annual volume of traffic sent for each sender ID and providing this data to the ACMA?

Record keeping and privacy

We propose that all participating telcos will be required to keep and maintain accurate records to demonstrate compliance with the standard, including to meet reporting and complaints-handling obligations referred to above. Participating telcos will be required to take reasonable steps to protect these records and have processes and systems to securely dispose of records when they are no longer required.

Participating telcos will also be required to follow applicable privacy obligations (in circumstances where the *Privacy Act 1988* does not apply) when handling personal information in connection with the register, such as during the registration process or when handling complaints.

The proposed rules that will apply to participating originating, transiting and terminating telcos are set out in the draft standard.

Question 29
Should any additional obligations for the register be included for specific/all participating telcos for:

- reporting
- record keeping
- traceback
- complaints handling?

System security

We propose to require participating telcos to take reasonable steps to secure their systems and processes to protect the integrity of the operation of the register, including in interactions with the register and entities that have registered sender IDs. This means that controls need to be in place and monitored to avoid systems and processes in the operation of the register being compromised by bad actors.

If a participating telco becomes aware of a security issue, it must provide details of the incident to the ACMA as soon as practicable, including the steps it has taken to rectify the matter.

These obligations recognise that interactions between a telco's systems and the register create a potential point of vulnerability that bad actors may attempt to exploit to:

- compromise the effectiveness of the register, including by bypassing the operation of the register and sending unauthorised sender ID messages
- corrupt or misuse information on the register
- cause harm to Australian consumers and entities.

Register implementation

We must make a standard for the register by no later than 30 June 2025. That standard must be implemented in full by no later than 15 December 2025 and set out mandatory rules for telcos.

We propose staged implementation of the standard, as shown in Table 2, to allow time for telcos to prepare for the register and initiate registration of sender IDs before protections start.

Table 2: Register implementation dates and stages

Date	Stage
By 30 June 2025	The standard is made by the ACMA.
28 July 2025	Telcos can begin applying to the ACMA for approval to participate in the register, and onboard if approved. Sections 1-7, Part 4 and Part 6 of the standard commence.
1 October 2025	Rules in the standard about providing information and the registration process come into effect (Sections 8 to 11, paragraph 12(b) and Schedule 1 commence). Participating originating telcos will be required to contact entities that have existing arrangements to send messages with sender IDs to advise them about the register and offer to initiate registration (see 'Telco-initiated registration' section above). Registering sender IDs before the register begins will avoid disruption of legitimate sender ID messages.
15 December 2025	The standard comes fully into effect and disruption of unregistered sender IDs begins.

It is important that entity registration begins before the register protections start. If only a small number of sender IDs are registered (for example, 5%) when the register starts, it would result in the disruption of messages for a large number of sender IDs (the 95% that are unregistered). This may be a poor outcome for entities and consumers alike.

Delaying the start of protections is also needed to educate entities and consumers about how they will be affected by the register.

Question 30
Are the proposed staged implementation timeframes appropriate and achievable? If not, what alternative approaches may be available, noting a standard must be made by 30 June and commence in full by 15 December 2025?

Issues for comment

We are seeking views from stakeholders, particularly from the telecommunications industry and entities, to help inform the design, implementation and operation of the register.

The questions listed throughout this paper are compiled below for ease of reference. We also welcome feedback on any of the issues covered in the paper and the draft standard, including the proposed definitions.

Question 1
Are there any other requirements that the participant application process should include?

Question 2
Excluding overseas entities, will the requirement to cross-reference entities against the ABR prevent or impede any sector of the Australian market that uses sender ID messages from participating in the register?

Question 3
Will requiring entity accounts to be set up/approved by entity representatives listed on the ABR be a barrier to participation? If so, how can this be overcome without compromising the registration requirements?

Question 4
Should the register only allow entities with an Australian presence (that is, an ACN and/or ABN) to participate in the register? If yes, what would be the likely impact of disrupting international messages that use sender IDs?

Question 5
Do you propose any alternative approaches to allow international entities to participate that still meet the register objectives and do not compromise the effectiveness/security of the register? For example:

- Could there be arrangements which allow an Australian telco or entity to act as a proxy for an international entity for the purposes of the register?
- Should these arrangements be limited to certain types of international entities? If so, which types?
- How would any such arrangements be secure and prevent bad actors from registering sender ID associated with scam communications?
- Where should compliance obligations rest given the ACMA does not have jurisdiction over foreign telcos or entities?

Question 6
Do you support telco-initiated registration? Please explain your reasons.

If yes, is the ACMA's proposed approach (where originating telcos initiate registration but entities must confirm) suitable/workable?

Question 7
If you are an originating telco, do the instructions at Appendix B raise any issues for you?

Question 8
What types of circumstances or behaviour do you consider should cause the ACMA to consider revoking an entity's approval and how would the ACMA become aware of it?

Question 9
Should any additional symbols (e.g. '!' '#' '%' '?') be permitted for sender IDs?

Question 10
Should there be any other format limitations for sender IDs?

Question 11
Should the register be case sensitive (that is, lowercase and uppercase letters are required to match exactly)?

Question 12
Should there be a limit on the number of sender IDs that can be registered by an entity? If so, what should that limit be?

Question 13
Do you agree that the same sender ID could be used by multiple entities, provided each entity can establish a valid use case? Please explain your reasons.

Question 14
Is the ACMA's proposal to require sender IDs to be directly associated with an entity's name or a brand name workable? Do you agree this approach helps prevent the registration of spoofed/misleading/deceptive/generic sender IDs? Please explain the reasons for your response.

Question 15
What alternative measures could be taken to confirm an entity has a valid use case for a sender ID?

Question 16
Are there other circumstances where the ACMA should remove sender IDs from the register?

Question 17
Is within 24- (or 48-) hours after 11.59 pm on the day a sender ID is registered an appropriate amount of time for telcos to update their systems with sender ID data? Would another period be preferrable? Please provide detail to support your response.

Question 18
Do you have any comments or concerns about how originating, transiting, and terminating telcos are defined?

Question 19
Are the proposed obligations for originating, transiting, and terminating telcos appropriate?

If not, what would prevent each type of telco from meeting the proposed requirements?

What exceptions should be included?

Question 20
The proposed model requires messages with sender IDs to only be sent, transited or terminated by telcos participating in the register. Does this model pose any issues and, if so, what, for:

- telcos
- EMSPs
- entities?

Question 21
Is the proposal for terminating telcos to over-stamp unregistered sender IDs required and/or supported? We are interested in views from across the sector, including those of terminating telcos.

Question 22
Does the solution overview proposed at Appendix A raise any issues for telcos?

Question 23
Noting that:

- the ACMA proposes only participating telcos can receive messages with sender IDs, and
- only Australian telcos can participate in the register,

should arrangements be implemented to allow the receipt of sender ID messages from an international (and therefore non-participating) telco? For example:

- could an Australian telco who receives sender ID messages from international telcos be considered an originating telco and be required to validate the sender ID (as set out in the 'Originating telcos' section above)
- how would such an arrangement work? Are there any alternative approaches that would meet the register objectives and would not compromise the effectiveness or security of the register?

Question 24
The ACMA is proposing that only participating telcos will be permitted to send, transit and terminate messages with sender IDs, which effectively blocks messages from non-participating telcos. Should messages from non-participating telcos be over-stamped instead? Please explain your reasons.

Question 25
Given the risks and benefits of over-stamping versus blocking, do you agree with the ACMA's graduated disruption approach − to initially over-stamp unregistered sender IDs and subsequently consider blocking?

Are there other disruption options or transitional arrangements that should be considered?

Question 26
If unregistered sender IDs are over-stamped rather than blocked, what term should be used − 'Likely SCAM', 'unverified', or something else?

Question 27

Is there any other information about the register telcos should be required to report to the ACMA?

Do telcos have a preference for how these reports should be provided, for example automated or API reporting?

Question 28

Are there any obstacles to originating telcos collecting data on the annual volume of traffic sent for each sender ID and providing this data to the ACMA?

Question 29

Should any additional obligations for the register be included for specific/all participating telcos for:

- reporting
- record keeping
- traceback
- complaints handling?

Question 30

Are the proposed staged implementation timeframes appropriate and achievable? If not, what alternative approaches may be available, noting a standard must be made by 30 June and commence in full by 15 December 2025?

Invitation to comment

Making a submission

We invite comments on the issues set out in this consultation paper.

- Submissions in PDF, Microsoft Word or Rich Text Format are preferred and can be emailed to senderIDregister@acma.gov.au
- Submissions by post can be sent to:

  Silvia Superina
  Scam Reduction
  Australian Communications and Media Authority
  PO Box 13112, Law Courts, Melbourne VIC 8010

The closing date for submissions is COB, **Monday 28 April 2025**.

Consultation enquiries can be emailed to senderIDregister@acma.gov.au

Publication of submissions

We will not publish submissions but may share them with the Department and the Minister for Communications' Office.

Confidential information will not be published or otherwise released unless required or authorised by law.

Privacy

View information about our policy on the publication of submissions, including collection of personal information during consultation and how we handle that information.

Information on the *Privacy Act 1988*, how to access or correct personal information, how to make a privacy complaint and how we will deal with any complaints, is available in our privacy policy.

Appendix A: Solution background

The voluntary SMS sender ID register pilot, launched in December 2023, relies on firewall rules on mobile networks to protect sender IDs subject to scammer impersonation. These rules work by blocking registered sender IDs that do not originate from the user of the sender ID's (single) telco.

The firewall rules approach offers immediate benefits but cannot protect all sender IDs or be efficiently or effectively scaled to address an ecosystem-wide solution, including because entities send sender IDs from more than one telco, and different entities may use the same sender ID.

To address these limitations, the ACMA is proposing to implement a register where protections begin before origination of messages. In this approach, as part of the registration process, the register will verify:

- the identity of the person who contacted the telco seeking registration
- that the entity the person represents is a legitimate entity
- that the person is an authorised representative of that entity.

Originating telcos will be required to verify that the entity has a valid use case for a sender ID before it can be registered.

Originating telcos will then use the register to verify that a sender ID is registered before sending SMS/MMS messages with sender IDs. The originating telco must disrupt messages with unregistered sender IDs by over-stamping the unregistered tag with 'Likely SCAM' before sending messages.

The ACMA is proposing to implement a sender ID registration and verification process that complies with the Rich Communication Services (RCS) standard to avoid implementing a bespoke standard just for the Australian market.

The ACMA understands that the introduction of the RCS standard on telco networks is a matter for the telcos, and Apple and Google can use the RCS standard over the top of telco networks. The ACMA's proposal to use RCS is limited to the Application Programming Interface (API) – essentially mechanisms that enable 2 software components to communicate with each other using a set of definitions and protocols – of the register and does not require or rely upon the implementation of RCS within telco networks. The ACMA does intend the register to evolve with messaging standards and believes the use of the RCS standard minimises future compatibility risk.

The RCS sender verification process involves originating telcos using verification authorities to verify their customers and the sender IDs (referred to as chatbots in the RCS standard). The standard mandates that verification authorities implement a standard API. This API allows originating telcos to initiate the verification of their customers and sender IDs and receive notifications about the verification outcomes, thereby facilitating a telco-initiated registration and verification process that could also be applicable to SMS/MMS using sender IDs.

Introducing a register that aligns with and leverages the RCS sender verification process positions the register for the future. It is intended that integration effort for telcos is reduced

and avoids the limitations of a custom solution. It will enable the register to support the verification of RCS messages in the future.

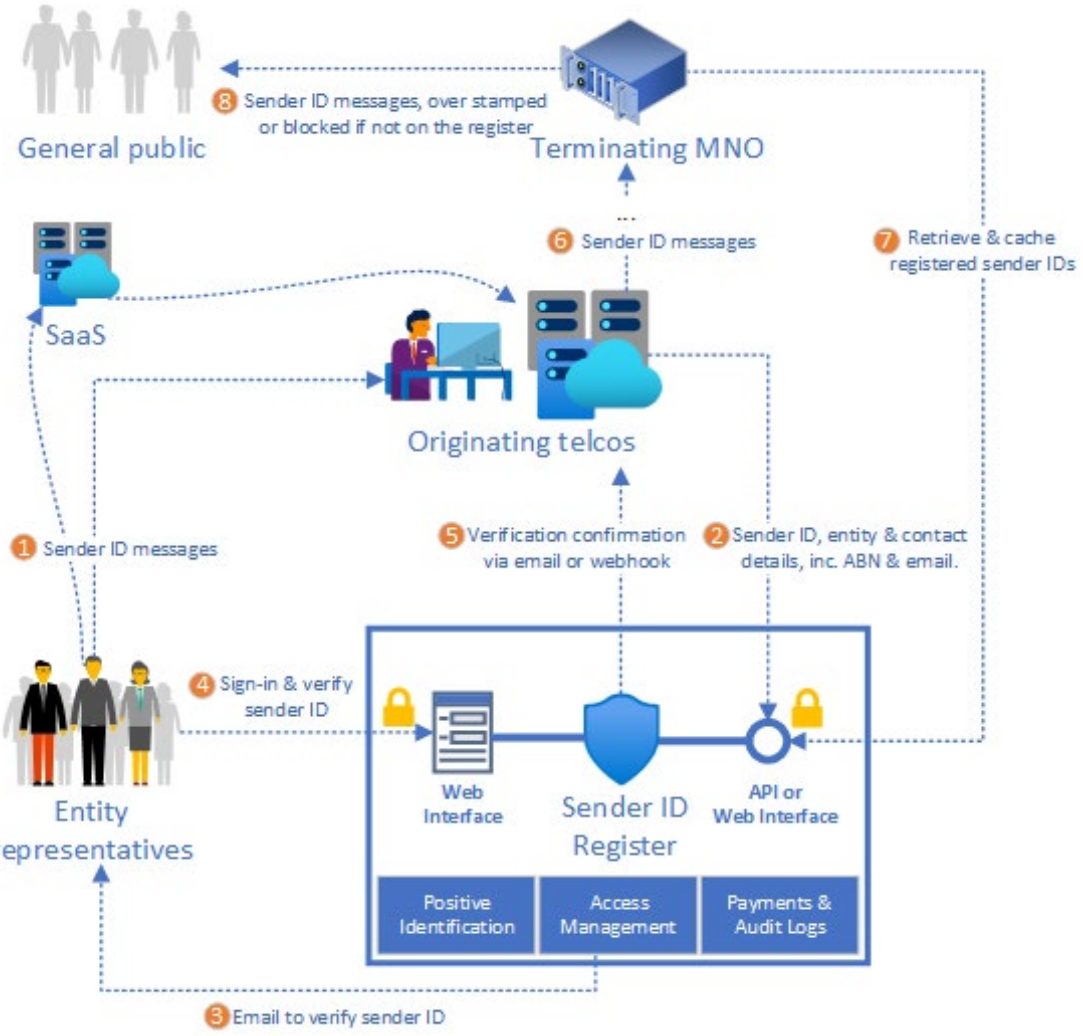
Overview

The register will facilitate a telco-initiated sender ID registration and verification process by implementing:

- A secure API and web interface for originating telcos to submit information on sender IDs, entities, and entity representatives intending to use those sender IDs. This information includes an entity's ABN and the representative's email address so that the register can email instructions and a link to complete the sender ID verification process.
- A secure web interface where entity representatives can:
  - sign in or sign up following successful identification through a document verification process
  - prove their authorisation as representatives either by signing in with the email address listed as an authorised contact for the entity according to the ABR, or by requesting access through authorised contacts
  - pay any registration fees
  - verify (or revoke) the use of the sender ID by the originating telco, enabling the register to notify the originating telco that they are now authorised to use (or can no longer use) the sender ID. Notifications are sent either directly to the originating telco systems or by emailing the configured mailbox.
- A secure API provided to terminating Mobile Network Operators to access the registered sender ID list, allowing them to disrupt sender IDs that are not on the register.

Figure 6 illustrates how the register proposes to streamline and support the entire sender ID registration and verification process, if over-stamping is the disruption method.

Figure 6: Sender ID registration and verification process in the SMS sender ID register using over-stamping



As illustrated in Figure 6, entity representatives will engage directly with originating telcos or third-party EMSPs (such as SaaS providers) to setup their SMS/MMS messaging. The originating telcos are responsible for establishing a valid use case for the use of sender IDs, submitting and awaiting the verification of the sender IDs before allowing the messaging to proceed. Until the sender ID is verified (that is, registration is confirmed by the authorised entity representatives and approved by the ACMA), originating telcos must disrupt messages from unverified sender IDs by over-stamping them with ‘Likely SCAM’.

Originating telcos can submit and initiate verification of the sender IDs through their own systems integrated with the register via API or by using the register web interface. Both the API and web interface will support sender ID registration/verification processes on behalf of partners, such as EMSPs, using originating telcos to send SMS/MMS messages.

The register will facilitate access management, enabling originating telcos to authorise their staff to use the web interface or their systems to call the API.

After a sender ID is submitted for verification, the register will send instructions and a link to the web interface to the entity representative to complete the verification process.

If the business representative has not signed up for the register, they will need to create an account by confirming their email address and completing the document verification process online. Alternatively, they can use Digital ID to sign in.

The register will use the ABR to check whether the email of the signed-in user is on the authorised contact list of the entity according to ABR. If it is, they can proceed to verifying the sender IDs. Otherwise, they will be given the option to specify and confirm an alternative email address that appears on the ABR authorised contact list or follow instructions on how to locate and request access from the authorised contacts.

If the entity has not paid any required registration fees, the entity representative would be required to pay those fees before verifying a sender ID. This can be done either by credit card or by downloading and paying the invoice using EFT.

After a sender ID is verified by an entity's authorised representative, the register will inform the originating telco's system(s) via API callback and/or email to the configured mailbox. This notification allows the originating telco to enable messaging from the verified sender ID. If a sender ID is not registered, the originating telco will be required to disrupt the message by over-stamping the unregistered sender ID before sending messages.

Terminating Mobile Network Operators will periodically (within 24- or 48-hours – see the 'Overview of proposed telco rules' section) download a list of verified sender IDs from the sender ID via API. They will use this list to over-stamp sender IDs that are not registered. Mobile Network Operators, as transiting telcos, will not be required to disrupt messages with registered sender IDs sent to overseas mobile numbers roaming in Australia.

The register will maintain an audit log to record the activities of all participants, supporting compliance and enforcement processes, and monitoring the effectiveness of the register.

Appendix B: Registration instructions for originating telcos

This appendix sets out the process originating telcos will be required to follow when they offer to initiate registration of a sender ID on behalf of an entity (in accordance with paragraphs 8(1)(a), 8(2)(c), 8(3)(c) and section 9 of the draft standard). The obligations to provide information before starting this process are covered in paragraphs 8(1)(a), 8(2)(c) and 8(3)(c) of the draft standard.

1. If an originating telco has offered to initiate registration of a sender ID (as required under 8(1)(b), 8(2)(d) and 8(3)(d) of the standard) and the representative says:
   a) they **agree to register** − go to item **2**
   b) they **don't agree to register** − go to item **3**
   c) the sender ID is **already registered** (e.g. via another telco), go to item **4**.

2. **Agree to register** – The originating telco must obtain the following information from the representative and (with consent) enter it into the register. *Note: this information may need to be entered in 2 steps: first items a, b, and c, and subsequently item d*.
   a) **Entity name and ABN** − The register will check this information against the ABR. The register will not allow registration to proceed if this information is not valid.
   b) **Sender ID** − The register will check if the sender ID meets registration requirements (for example, length, types of characters used). The register will not allow registration to proceed if the sender ID does not meet these requirements.
   c) **Entity representative name and email address** − The register will check whether the representative is authorised (that is, if they are listed on the register as a business administrator or authorised representative for that entity) . If the person isn't authorised, the register will provide instructions about how to obtain authorisation.
   d) **Confirmation of a valid use case** − evidence demonstrating the sender ID is directly associated with the entity. Registration cannot proceed without a valid use case. *Note: the telco would have to check a box in the register confirming it has assessed the entity has a valid use case. The evidence does not need to be entered into the register, but the originating telco is required to keep records to demonstrate it has complied with this requirement*.

   If the application is accepted, the register will notify the originating telco via email that the application status is 'pending'. Go to item **5.**

   The originating telco must advise the representative that they will receive notification from the register, which will include instructions about how to access the register so they can confirm the registration request. The request must be approved before the originating telco can send sender ID messages for the nominated sender ID.

3. **Don't agree to register** – The originating telco must advise the representative that unregistered sender ID will be over-stamped.

4. **Sender ID is already registered** – The originating telco must obtain the following information from the representative and enter it into the register:
   - entity name and ABN
   - sender ID
   - their name and email address.

   The register checks if the nominated sender ID is registered for *that* entity (noting that more than one entity may register the same sender ID):
   a) If yes (the sender ID is registered), the register will send a notification to the entity representative asking them to confirm that the originating telco is authorised to send messages using the registered sender ID. (Note: the originating telco does not need to establish a valid use case in this case, as this would have been done when the sender ID was first registered). Go to item **5**.
   b) If **no** (it isn't registered), but the representative would like to register, go to item **2**. If **no**, and the representative doesn't want to register, go to item **3**.

After registration request is accepted by the register

5. The register sends an email to the representative with a link to the register, asking them to confirm:
   a) **If sender ID was not previously registered** − registration of the sender ID and that the originating telco is authorised to send messages using that sender ID
   b) **If sender ID already registered −** that the originating telco is authorised to send messages using that sender ID.

   The register will also send information to the entity about how to use the register and any register fees.

6. The representative accesses the register. This requires them to sign up to ACMA Assist (if they haven't done so already) and undergo ID verification (confirming they are a real person) and agree to the register terms and conditions. If the entity/sender ID is not already registered, the entity will be prompted to pay any upfront fees that may apply.

7. The register checks that the representative is listed as a business administrator or authorised representative for that entity. If the representative is not authorised, the register provides instructions on obtaining authorisation, which includes contacting or locating administrators for the business.

8. Once the register confirms the representative is authorised by the entity, the representative can confirm or reject via the register the:
   a) request to register a sender ID
   b) request to authorise an originating telco to send messages using a registered sender ID.

9. Upon verification, the register notifies the originating telco that the sender ID can now be used, allowing them to send messages using the registered sender ID. If the originating telco receives notification the request has been declined, it **cannot** send messages using that sender ID. The originating telco must over-stamp the sender ID before sending messages.

10. Once a sender ID is verified for use with an originating telco, the verification remains in place until revoked by the entity. A sender ID can be verified for use with multiple telcos.