SMS Sender ID Register

28 April 2025

Recommendations

This Submission recommends the Australian Communications and Media Authority:

1. Prioritise positive consumer outcomes through the consistent application of the SMS Sender ID Register.
2. Introduce more stringent requirements for telecommunication providers to establish an entity's valid use case.
3. Ensure a sender ID must only be registered to a single entity.
4. Develop a robust, secure and accountable proxy arrangement to allow for the participation of international entities and telecommunication providers.
5. Limit the number of sender IDs that can be registered by a single entity.
6. Remove sender IDs from the register if the sender ID has not been used by the entity in the past two years.
7. Adopt a proactive and comprehensive role in the design, implementation, and ongoing management and enforcement of the SMS sender ID register.

About this submission

The Australian Communications Consumer Action Network (ACCAN) is pleased to provide this submission to the Australian Communications and Media Authority (ACMA) regarding the Telecommunications (SMS Sender ID Register) Industry Standard 2025 (the Standard) and proposed register operation. ACCAN welcomes the ACMA's focus on protecting Australians from SMS scams through the development of the Standard. ACCAN's submission is endorsed by Consumer Action Law Centre.

Contents

ACCAN is the peak national consumer organisation advocating for fair communications and digital services.

Introduction

The introduction of a mandatory SMS Sender ID Register (the register) in Australia presents a critical opportunity for the law to disrupt scam business models and ensure Australian consumers are protected from harm. ACCAN supports the Government's objectives for the register to disrupt unregistered sender IDs, protect consumers against spoofing sender IDs, promote public confidence in sender IDs, and promote consistency and accountability of industry actions in relation to sender ID communications.[1]

If appropriately implemented, the register can lead to a significant reduction in the number of SMS impersonation scams and the financial losses attributable to these scams. Impact analysis of a mandatory SMS Sender ID Register scheme in Australia found the net benefit to consumers and businesses over 10 years to be $96.2 million.[2] The introduction of a SMS sender ID register in Singapore led to a 64% decrease in reported SMS scams.[3] 87% of consumers agreed the register made it easier to identify the legitimacy of the SMS they receive.[4]

To promote positive consumer outcomes, ACCAN considers the Standard must clearly set out obligations on participating telecommunication providers, promote uptake of the register, and ensure consistent implementation across the telecommunications sector. As scammers will evolve and adapt their business models, ACCAN considers the ACMA must be flexible, proactive and responsive to ensure the register remains fit for purpose and meets the objectives set out in the Telecommunications (SMS Sender ID Register Industry Standard) Direction 2025 (the direction). ACCAN supports the ACMA conducting a comprehensive assessment of the register 12 months after its full implementation and making that assessment public.

This submission sets out the prevalence and harm caused by SMS impersonation scams in Australia and ACCAN's key concerns and responses to the questions outlined in the consultation paper.[5]

[1] Telecommunications (SMS Sender ID Register Industry Standard) Direction 2025 (Cth) s 7.
[2] Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Fighting SMS impersonation scams: the SMS Sender ID Register model for Australia (Impact analysis, November 2024) 44 ('DITRDCA Impact Analysis').
[3] Infocomm Media Development Authority, 'Full SMS Sender ID Registration is to be required by January 2023' (Media release, 17 October 2022) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2022/full-sms-sender-id-registration-to-be-required-by-january-2023>.
[4] 'Singapore Consumers More Confident in Recognising Scams: Toku Research', PR Newswire (online, 16 November 2023) <https://www.prnewswire.com/apac/news-releases/singapore-consumers-more-confident-in-recognising-scams-toku-research-301989934.html>.
[5] ACMA, SMS sender ID register: Consultation on a draft industry standard and proposed register operation (Consultation paper, March 2025).

Background

SMS scams are rampant in Australia. Between July 2022 and December 2024, telecommunications providers reported blocking 857.4 million scam SMS.[6] In 2023, text message scams cost Australians $26.9 million.[7]

SMS scams frequently impersonate trusted businesses, organisations or government agencies to gain money or access to a victim's personal information. Impersonation scams accounted for more than 70% of the 234,672 reports to Scamwatch between 1 January and 30 September 2023 and cost Australians $92 million.[8]

SMS impersonation scams use fraudulent sender IDs to deceive victims and account for 55% of all SMS scams received.[9] Further Scamwatch data from January to July 2024 found 79% of text message scams involved impersonation.[10]

The true extent of harm suffered as a result of SMS scams is difficult to estimate due to persistent underreporting. Research conducted by Deloitte Access Economics found 70% of consumers experiencing financial losses from SMS scams did not report the scam to Scamwatch.[11] Australian Bureau of Statistics data also found less than 1 in 10 scammed Australians reported it to a government department in 2023-24.[12]

SMS scams cause considerable consumer detriment beyond financial harm. Scam victims often report significant emotional and psychological distress and other ongoing harms. Deloitte Access Economics estimated the total cost to consumers for SMS scams, including losses, time spent to resolve scams, and nuisance cost to be $192 million.[13]

By establishing a centralised system that verifies the legitimacy of sender IDs and prevents spoofing, the register offers a much-needed mechanism to dismantle a key tactic employed by scammers, thereby significantly reducing the potential for such large-scale and insidious impersonation scams to succeed.

[6] ACMA, Action on scams, spam and telemarketing: October to December 2024 (Report) [3].
[7] Tom Stayner, Alex Anyfantis, 'The days and times you're most likely to receive a scam text in Australia', SBS News (online, 29 June 2024) <https://www.sbs.com.au/news/article/the-days-and-times-youre-most-likely-to-receive-a-scam-text-in-australia/9idp6670t>.
[8]Australian Competition & Consumer Commission, 'Scams Awareness Week 2023 empowers consumers to ask "Who's really there?"' (Media release, 147/23, 30 November 2023) [1] <https://www.accc.gov.au/media-release/scams-awareness-week-2023-empowers-consumers-to-ask-whos-really-there>.
[9] DITRDCA Impact Analysis 34.
[10] Ibid. The 79% figure is derived from data on page 34 that outlines 'between the period of 1 January and 31 July 2024, Scamwatch received 63,121 reports where the scam contact mode was listed as 'text message' (SMS). Of those, 50,062 reported scams involved 'impersonation".
[11] Ibid.
[12] Australian Bureau of Statistics, Personal Fraud (Report, 2 April 2025) <https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release#scams>.
[13] DITRDCA Impact Analysis 54.

The numerous media reports of sophisticated SMS spoofing scams, which have defrauded Australian consumers hundreds of thousands of dollars, underscore the acute danger posed by sender ID impersonation.[14] The prominence of Australian Securities and Investment Commission's lawsuit against HSBC in December 2024 exemplifies this threat. The legal action arose from HSBC's failure to protect customers from a long-running scam that stole $23 million from consumers over nearly five years.[15] The spoofing scam used a fraudulent sender ID, so messages appeared in the same text chain as legitimate HSBC communications.[16] This ability to easily impersonate trusted entities through sender ID manipulation has contributed to significant consumer harm, leaving victims with no or limited recourse to reclaim their scammed funds, despite businesses, including those delivering essential services, being on notice of this activity for some time.

Consumer Action Law Centre case study – Chris's story

In June last year Chris received a text SMS from his phone service provider, a few days after he had visited their store and made a purchase. The SMS said that he had earned points on his purchase which he could redeem on products by following a link. It appeared in the same thread as other texts from his provider.

After selecting a product slightly more expensive than the points he had earned, Chris entered his credit card details to pay for the remaining amount.

Chris's card was charged several thousand dollars to an overseas business. He realised it was a scam and immediately called his bank's fraud team to report the fraudulent transaction. They said they couldn't do anything while the transaction was pending, and they would have to let it go through.
When the transaction cleared, Chris requested a charge back – but the bank said they couldn't do that because the transaction was unauthorised – although that it wasn't eligible for reimbursement under the ePayments Code.

After raising a complaint at AFCA, Chris's bank offered less than half of what had been charged as a goodwill payment.

**Not his real name*

Amy's* story – Financial Rights Legal Centre (S305628/S308740)

Amy received a spoofed text message on the same chain as her legitimate bank messages, asking her to contact a number if she had not requested a verification code (which she had not).

Once Amy called the number, and someone explained that multiple devices attempting to access her account, and it needed to be blocked. Amy gave her username and some verification codes to the scammer and proceeded to get locked out of her account and have a new device, not belonging to her, granted access to her account. The scammer changed Amy's daily payment limit and over $45,000 was debited out of Amy's account into another account with the same bank, without Amy's knowledge or consent. As the funds were quickly moved again and then withdrawn, they could not be recovered.

Amy's bank was unable to detect and block the transaction, even though there was a login from a completely new device, with an instant change in daily payment limit and instant transfer of a large lump sum to a new account. The bank also continues to use SMS for communication, knowing that this has been compromised due to various fraud victims' cases in the past. There were no safeguards available to suspend suspicious transactions.

The bank withheld compensation in part in reliance on ineffective warnings, including:

(a) a broadcast "scam warning" SMS sent to customers before Amy became a customer, and

(b) SMS warnings that provided an OTP code and requested the customer to call the bank if not requested, but did not explicitly tell customers not to disclose the OTP code to the bank.

**Not her real name*
*** This case study was provided in the joint consumer submission submitted for the Scams Prevention Framework – exposure draft legislation, Federal Treasury consultation, as at 4 October 2024 and has not been updated.[17]*

[17] Consumer Action Law Centre et al, Submission to The Treasury, Scams Prevention Framework – exposure draft legislation (4 October 2024) 52.

Ishan's* story – Financial Rights Legal Centre (S305251/ S305548)

Less than a year ago, Ishan received a spoofed text message on the same chain as his legitimate bank messages, providing a verification code and asking him to contact a number if he had not requested a verification code. As Ishan had not requested a code, he rang the number and the person who answered identified him in accordance with the bank's usual procedures. The person told Ishan two devices were attempting to access his account, and requested Ishan provide One Time Passcodes (OTP) to remove and block the unauthorised devices. Ishan did this, and the scammer used these codes to block his access to the account, link a new device, and transfer almost $50,000 from Ishan's account into another account with the same bank (then quickly out and overseas thereafter).

In response to a "suspicious activity alert" email from his bank after the transfers had taken place, Ishan rang his bank's call centre, and the bank identified Ishan was the victim of a scam. It was unable to recover any of his money.In refusing Ishan's request for compensation, the bank relied on various warning messages it had sent to Ishan, including generic broadcast SMS and emails about scam risk generally, as well as the warnings which accompanied the OTPs when Ishan generated them in the bank app and then unwittingly provided to the scammer. While Ishan acknowledged he may have received the generic communications, he denied having received the transaction-specific warnings; further, he said that the "warning" not to share OTPs with bank staff was inconsistent with previous practice by the bank, where this was routine.

During the course of Ishan's AFCA complaint, a significant amount of additional information was disclosed by the bank about its internal processes while the scam was taking place, including that no OTP was required when the scammer changed Ishan's online account password, that the bank's records were inconsistent as to whether an OTP was or was not required to set up the new payee (the scammer), and that the bank identified the transaction as a potential scam and suspended both his and the receiving account, but did not inform Ishan other than to send a fairly bland email requesting he contact the bank. Whether these matters will impact the outcome in Ishan's case is unknown, as the matter is still before AFCA.

**Not his real name*
*** This case study was provided in the joint consumer submission submitted for the Scams Prevention Framework – exposure draft legislation, Federal Treasury consultation, as at 4 October 2024 and has not been updated.*

[18] Ibid 22.

Key concerns

ACCAN considers that the robust initial implementation of the register is vital for the register to successfully meet its intended objectives in promoting confidence in SMS communications. Any vulnerabilities or exploitable loopholes allowed within the register would result in a number of detrimental outcomes. First, businesses and consumers may experience a complete erosion of trust in the register's reliability as a source of legitimate information. Secondly, and more critically, individuals may be susceptible to scams after placing confidence in the register's purported integrity, thereby undermining its fundamental purpose of consumer protection. Consequently, a flawed initial implementation carries significant risks that could negate the register's intended benefits.

ACCAN's feedback in this submission focuses on the role of the register in promoting positive consumer outcomes. Positive consumer outcomes in this instance include:

- Consumers can confidently trust the legitimacy of SMS communications, without needing to rely on digital literacy skills to determine if an SMS is legitimate.
- Consumers can readily and accurately identify the sender of the SMS.
- Communications to consumers are not unnecessarily disrupted, so consumers can access information they require from legitimate senders of SMS.
- A reduction in financial losses attributable to SMS scams and a reduction in the number of reported SMS scams.

Entity registration

Fraudulent companies are a pervasive problem in Australia and recent enforcement action by ASIC against 95 companies highlights the extent of the issue.[19] The case shows that scammers are using advanced methods to bypass current ID checks, incorporating companies using false information and creating professional-looking online presences to appear legitimate. ASIC Deputy Chair stated in the media release that 'these scams are like hydras: you shut down one and two more take its place'.[20]

To address issues like false director identities and illegal phoenix activity, reforms to the Corporations Act 2001 that took effect in 2021 introduced a requirement for company directors to obtain a director ID.[21] While there isn't much public data yet to evaluate the success of these reforms, ASIC's recent enforcement actions strongly suggest that fraudulent companies remain a significant problem in Australia.

[19] Australian Securities and Investments Commission (ASIC), 'ASIC warns of threat from "hydra-like" scammers after obtaining court orders to shut down 95 companies' (media release, 7 April 2025) <https://asic.gov.au/about-asic/news-centre/find-a-media-release/2025-releases/25-052mr-asic-warns-of-threat-from-hydra-like-scammers-after-obtaining-court-orders-to-shut-down-95-companies/>.
[20] Ibid [8].
[21] 'New ID requirement for directors', ASIC (Web Page) <https://asic.gov.au/about-asic/news-centre/news-items/new-id-requirement-for-directors/>.

The clear, consistent and robust implementation of the SMS sender ID register is critical to promoting consumer confidence in SMS communications. ACCAN considers the requirements and implementation of the registration process must be stringent to capture fraudulent entities or individuals who seek to exploit the scheme, recognising that the register is reliant upon the robustness of other systems that regulate the establishment and registration of companies and directors more generally. In this regard, ACCAN has several key concerns regarding the registration process.

The Standard includes obligations on originating telecommunications providers to establish an entity's use case at section 10(2). The validity of a sender ID is proposed to be established by the originating telecommunication provider confirming that the sender ID is directly associated with or matches the entity's name or brand name and this is supported by documentary evidence.

ACCAN considers the requirements for providers to establish a valid use case as part of the entity registration process should be more prescriptive. The Standard does not set out a definition of entity name nor an entity's brand name. The Standard also lacks requirements regarding what is considered acceptable evidence that can be used to determine a valid use case of a sender ID under 10(a) and (b). We note the Standard offers an example of cross-checking with the Australian Business Register (ABR), but this is not a mandatory obligation.

As drafted, section 10 sets out broad obligations with little guidance on interpretation, allowing providers considerable discretion to determine the processes and evidence they rely on to establish a valid use case. This undermines the objectives of the Standard to promote consistency and accountability of actions taken by industry and increases the risk that the register will be exploited by fraudulent actors.
ACCAN recommends the ACMA clearly set out obligations regarding the cross-checking of an entity's use case. ACCAN recommends an Australian entity can only register an SMS sender ID if it matches one of the following:

- its registered business name as defined by the Business Names Registration Act 2011 (Cth)
- its company name as set out by the Corporations Act 2001 (Cth)
- its registered trademark as defined by the Trade Marks Act 1995 (Cth).

ACCAN considers that should an entity seek to register a sender ID not associated with one of the above, they are likely in breach of the Business Names Registration Act 2011 (Cth).

ACCAN supports the ACMA's proposal to verify the identity of sender ID applicants through the existing requirements to access the ACMA Assist portal but consider that some fraudulent entities may pass through undetected. ACCAN is concerned the ACMA's proposal to verify identity against the entity's authorised contacts listed on the ABR is limited to checking if the email address of the signed-in user matches that of an authorised contact. As email addresses are readily compromised, ACCAN supports the register undertaking stronger verification measures by checking the identity documents of the user match the name of a listed authorised contact on the ABR.

To guard the register against misuse, ACCAN recommends comprehensive reporting requirements on telecommunication providers to ensure the ACMA can take swift action to revoke registration of malicious actors.

Sender IDs registered to multiple entities

ACCAN strongly recommends a sender ID must only be registered to a single entity. The ACMA's proposal to allow multiple entities to register the same sender ID undermines the objectives of the register, leading to considerable consumer confusion and further mistrust of SMS communications. To this end, ACCAN considers that the ACMA must also consider if a sender ID is too similar to another registered sender ID when approving an application.

Should the ACMA adopt our recommendation to restrict sender IDs to be registered to only one entity, ACCAN considers there needs to be a limit on the number of sender IDs that can be registered by an entity. This will help ensure anti-competitive behaviour is not proliferated through entities 'buying up' other SMS sender IDs to restrict other entities that share a business or corporation name. We set out our recommendations regarding limiting sender IDs in our response to Question 12.

Responses to consultation questions

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

As set out earlier in the submission, ACCAN considers the ACMA must introduce more stringent requirements on telecommunication providers to establish an entity's valid use case of a sender ID.

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?

ACCAN considers it appropriate that entities and their representatives are cross-referenced against the ABR.

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?

Alternative approaches to allow international entities to participate in the SMS sender ID register are possible and should be explored, provided they rigorously uphold the register's objectives, do not compromise its effectiveness or security, and promote positive consumer outcomes.

ACCAN considers allowing international entities to participate in the register will promote positive consumer outcomes ensuring consumers are not blocked from receiving legitimate communications they may need.

This is particularly relevant for Australia's migrant population. In 2023-24 alone there were 667,000 total migrant arrivals.[22] Migrant populations may rely on SMS sender ID notifications from government agencies, bank accounts or financial services while they are in Australia. If the register were to block these SMS, it would effectively cut off migrant consumers from important and legitimate communication.

A carefully considered proxy arrangement, coupled with strict limitations and robust security measures, could facilitate legitimate communication from international entities while safeguarding consumers from SMS impersonation scams. We propose a tiered proxy arrangement involving Australian-based entities acting on behalf of international senders. An Australian telecommunications provider or a specifically accredited Australian entity (proxy provider) would register the international sender's desired SMS sender ID on their behalf. This proxy provider would be legally responsible under the Standard for the proper use of that sender ID.

Modelling on the principles and arrangements in *Australia's Anti-Money Laundering and Counter-Terrorism Financing* (AML/CTF) *Act 2006*, AML/CTF Rules and the accompanying AUSTRAC guidelines regarding correspondent banking provides a robust foundation that can guide the development of a proxy arrangement to facilitate secure international access to the register.[23] These regulations are relevant as they address the inherent risks associated with one Australian entity facilitating services or relationships with entities in another jurisdiction.

The principles embedded within AML/CTF Act and the guidance provided by AUSTRAC include the imperative for enhanced due diligence, requiring a thorough understanding and verification of the other party's identity, business, and risk profile.[24] These regulations emphasise a risk-based approach, mandating that entities identify, assess, and mitigate the specific money laundering and terrorism financing risks associated with their relationships.[25] Ongoing monitoring of transactions and activities is crucial to detect and report suspicious behaviour. Finally, the framework establishes clear lines of responsibility and accountability for regulated entities to ensure compliance and prevent their services from being exploited for illicit purposes.

[22] Australian Bureau of Statistics, Overseas Migration (Report, 13 December 2024) <https://www.abs.gov.au/statistics/people/population/overseas-migration/latest-release#cite-window2>.
[23] 'Core guidance', AUSTRAC (Web Page) <https://www.austrac.gov.au/business/core-guidance>; See more information regarding correspondent banking at 'Correspondent banking relationships', AUSTRAC (Web Page) <https://www.austrac.gov.au/correspondent-banking-relationships>. Regulations regarding correspondent banking are set out in Part 8 of AML/CTF Act 2006 and Chapter 3 of AML/CTF Rules.
[24] 'Anti-money laundering and counter-terrorism financing', Attorney-General's Department (Web Page) <https://www.ag.gov.au/crime/anti-money-laundering-and-counter-terrorism-financing#:~:text=Beyond%20that%2C%20each%20business%20must,designated%20service%20to%20a%20customer>.
[25] Ibid.

These principles collectively aim to create a system where regulated intermediaries act as gatekeepers, actively working to prevent the flow of illicit funds and maintain the integrity of the financial system. This alignment with the principles underpinning Australia's approach to managing risks in international financial dealings underscores the necessity of a similarly robust and accountable framework for enabling legitimate international participation in the SMS sender ID register without compromising its security or effectiveness in protecting Australian consumers from scams.

ACCAN considers access to a proxy arrangement to participate in the register should be strictly limited and Australian entities wishing to become a proxy provider must apply to the ACMA for approval. To verify a proxy provider, the ACMA would need to conduct a strict accreditation process that includes background checks and demonstrated history of compliance with obligations. Further, access to the proxy arrangement should be restricted to specific types of international entities that demonstrate a legitimate need to communicate with Australian consumers and can meet stringent verification assessments. Types of international entities could include:

- Entities operating within well-established and regulated industries in their home countries. For example, major financial institutions, airlines, government bodies, and educational institutions. Proof of regulatory compliance and registration in their jurisdiction would be mandatory.
- International entities with a significant and verifiable physical presence or subsidiary within Australia, subject to Australian law.
- International organisations providing critical services to Australian residents such as international health care providers or emergency services.

Access to a proxy arrangement should explicitly exclude entities based in jurisdictions with weak regulatory oversight or a high prevalence of cybercrime. ACCAN considers that sender IDs registered to international entities could be prefixed with a “#” tag to help consumers identify their international origin.[26]

ACCAN considers compliance obligations would primarily rest with the Australian proxy provider to ensure the ACMA has jurisdiction to prescribe and monitor compliance with registration rules. The proxy provider would be held legally accountable for ensuring the international entity they represent adheres to the terms and conditions of the sender ID registration and regulations. The proxy provider should be held liable for any misuse of the registered sender ID that results in harm to Australia consumers. Proxy providers should also be obligated to promptly investigate any reported misuse of sender IDs they have registered and take appropriate and immediate remediation actions, including suspending and/or terminating the arrangement with the international entity.

[26] Hong Kong operates a voluntary SMS Sender ID registration scheme where registered sender IDs are prefixed with a "#" tag. This prefix helps consumers identify that the sender ID is registered and legitimate, providing transparency and trust in SMS communications. See DITRDCA Impact Analysis 22.

ACCAN considers proxy providers would be legally obligated to conduct comprehensive due diligence on the international entities they represent prior to registering a sender ID on their behalf. This should include verifying their legal existence, ownership, operational legitimacy, and the purpose of their SMS communications to Australian consumers. Independent verification processes or third-party certifications could be mandated. Additional layers of security should include:

- Legally binding agreements between the proxy provider and the international entity that clearly outline acceptable use policies, prohibited activities (including sending unsolicited or scam SMS), data security requirements, and audit clauses.
- Technical safeguards embedded in the registration process to prevent unauthorised registration including verification of identity and multi-factor authentication.

The inclusion of international entities in the register necessitates a broader regulatory compliance and enforcement role of the ACMA. The ACMA would need to implement mechanisms for ongoing monitoring of proxy providers and the SMS traffic associated with the registered international sender IDs. Regular audits of proxy providers' due diligence processes and compliance with the terms of registration should be conducted.

In addition, proxy providers should be subject to comprehensive reporting requirements to ensure effective regulatory oversight of the register. At minimum, this should include:

- For each international entity they represent, proxy providers submit a comprehensive report to the ACMA including the entity's details, legal registration, services or activities it undertakes, and specific purposes or intended use of the SMS sender ID/s being registered.
- An initial risk assessment conducted by the proxy provider regarding the potential for misuse of the sender ID by the international entity.
- A thorough description of the due diligence process undertaken by the proxy provider to verify the legitimacy of the international entity, including the sources of information consulted and the steps taken.
- A periodic attestation by a senior officer of the proxy provider confirming that the international entity continues to meet the agreed-upon terms and conditions, and that the information provided in previous reports remains accurate.
- Immediate reporting of any suspected or confirmed instances of sender ID misuse, security breaches, or non-compliance by the international entity. This should include a detailed description of the incident, the steps taken to mitigate the impact, and preventative measures implemented.

ACCAN considers other reporting arrangements could include proxy providers supplying the ACMA with the following:

- A copy of the legally binding agreement (including any Service Level Agreements) between the proxy provider and the international entity, outlining responsibilities, acceptable use policies, and liabilities.
- Reports detailing the volume of SMS messages sent under each registered sender ID by the international entity, categorised by purpose (e.g. multi-factor authentication, informational, marketing)
- Prompt notification of any significant changes in the international entity's legal status, ownership, operational activities, or contact information.
- Immediate notification to the ACMA if the proxy provider terminates its agreement with an international entity, including the reasons for termination.

To ensure consistency and facilitate efficient data collection and analysis, the ACMA should provide standardised templates and formats for all the required reports. Reporting deadlines must reflect a risk-based approach that requires proxy providers to provide more frequent and detailed reports to the ACMA as their activities present a higher risk than that other register participants.

With stringent security measures and active enforcement, the participation of international entities with the register can offer several benefits to communication consumers. This proposal facilitates legitimate communication from international entities, ensuring consumers are not blocked from accessing information they require. Consumers can have greater confidence in SMS originating from registered sender IDs, even if facilitated through a proxy, knowing an Australian entity is accountable. By placing responsibility on Australian-based entities, the ACMA retains a clear point of accountability and enforcement. Proxy providers are therefore incentivised to comply with stringent verification and accreditation process due to their risk of liability.

Should the ACMA permit the participation of international entities, ACCAN considers the accreditation process for proxy providers must be robust and transparent. The due diligence requirements for international entities need to be clearly defined and consistently applied. The ACMA must set out clear legal frameworks and enforcement mechanisms to ensure proxy providers meet their obligations and the ACMA takes a proactive position in conducting ongoing review and adaptation of the model to address evolving threats and ensure its continued effectiveness.

By implementing a well-defined and rigorously enforced tiered proxy arrangement, the ACMA can potentially allow legitimate international participation in the SMS sender ID register without compromising its core objectives of enhancing consumer trust, security, and reducing SMS scams. The focus on Australian-based accountability and regulatory enforcement is paramount to the success of this approach.

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?

Given the critical importance of robust verification processes during registration to prevent the inclusion of malicious actors on the register, ACCAN considers ACMA is best placed to conduct the entire entity registration process rather than adopting the telco-initiated registration proposal. The benefits of the ACMA conducting the registration process include the regulator's ability to co-operate with ASIC regarding cross-referencing entities and a simpler user experience for entities to apply. However, ACCAN understands this may require significant ICT system changes and diverges from current industry practice.

If the ACMA adopts telco-initiated registration, it is critical the ACMA set out more stringent requirements for providers to establish a valid use case. ACCAN supports requirements for telecommunication providers to attach to the application on behalf of the entity, the evidence they relied upon to establish a valid use case (i.e. the entity's details on the ABR). ACCAN also supports the ACMA establishing processes to monitor and periodically review compliance with the Standard.

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?

ACCAN supports the ACMA revoking an entity's approval in any of the following instances where an entity:

- Is found to have provided information that is misleading or untruthful when registering.
- Is found to be proliferating scams or fraudulent messages using the sender ID.
- Breaches spam rules via the sender ID as set out by the *Spam Act 2003 and Spam Regulations 2001*.
- Has or is involved in scam activities.

ACCAN considers the ACMA will become aware of illegitimate entities using the register through consumer complaints to providers regarding the register. As the ACMA enforces spam rules, it should become aware of breaches through its regular compliance and enforcement activities including audits.

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.

ACCAN supports ACMA's proposal for sender IDs to be case-insensitive.
As outlined earlier in this submission, ACCAN has serious concerns regarding ACMA's proposal that multiple entities may use the same sender ID. SMS sent from two numbers with the same sender ID show up in the same message thread. This proposal will lead to considerable consumer confusion and undermines the Direction's objectives for the register to promote consumer confidence in SMS communications.[27]

ACCAN considers there should be a limit on the number of sender IDs that can be registered by an entity. Imposing a limit will curb anti-competitive behaviour and promote consumer confidence in identifying communications from a company if all messages are in one thread rather than delivered across several sender IDs. We agree with the benefits outlined in the consultation paper that 'limiting the number of sender IDs per entity may also help consolidate and reduce data recording and reporting requirements associated with the register'.[28] To account for entities having multiple brands, ACCAN considers an entity should be allowed to register a maximum of three sender IDs.

Should an entity seek to register several sender IDs, the ACMA may seek to impose higher registration fees to limit this practice.

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?

As outlined earlier in the submission, ACCAN considers the ACMA's proposal needs to go further to protect consumers and ensure the integrity of the register. ACCAN recommends more stringent requirements for providers to establish a valid use case to ensure the register is not exploited by scammers.

[27] Telecommunications (SMS Sender ID Register Industry Standard) Direction 2025 (Cth) s 7.
[28] ACMA, SMS sender ID register: Consultation on a draft industry standard and proposed register operation (Consultation paper, March 2025) 18.

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

ACCAN supports the ACMA proposal to remove offensive, misleading, deceptive, spoofed sender IDs or within other reasonable circumstances. ACCAN considers the ACMA should remove sender IDs from the register if the sender ID has not been used by the entity in the past 2 years.

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.

ACCAN supports the proposed time period of 24-48 hours for providers to update their systems according to register data. ACCAN considers any extension to this time period risks the unnecessary blocking of registered sender ID messages to consumers.

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?

ACCAN queries the consumer outcome if a provider chooses not to participate in the register. In this instance, ACCAN understands their customers would suffer from missing out on information that is received from registered sender ID messages due to the requirements on originating and transiting providers to only send sender ID messages to participating telcos (i.e. effectively blocking sender ID messages to non-participating providers).

ACCAN considers that to ensure uptake of the register among providers, the costs of the register should be proportionate and not prohibitive to ensure all consumers benefit, no matter their provider.

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?

ACCAN supports the proposal for terminating providers to over-stamp unregistered sender IDs and considers it is a vital safety net to ensure no unregistered sender IDs are terminated without including a warning to consumers.

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?

ACCAN considers arrangements should be implemented to allow the receipt of sender ID messages originating from international (and therefore non-participating) telcos, particularly in the context of the proposed tiered proxy arrangement. Our proposed model inherently addresses this question by establishing a mechanism for legitimate international entities to participate in the register indirectly through Australian proxy providers.

Under our proposed proxy model, an Australian telecommunications provider would receive SMS messages from international telcos. However, the key element is that the sender ID in these messages would have been registered in the register by an accredited Australian proxy provider acting on behalf of the international entity. Therefore, the Australian telco receiving the message would see the sender ID as registered within the Australian system.

The Australian receiving provider should be considered an originating telco for the purpose of validating the sender ID. Upon receiving a message with a sender ID associated with a proxy provider, the Australian provider would perform the validation checks as outlined in the 'Originating telcos' section of the ACMA's proposal. This validation would confirm that the sender ID is indeed registered and associated with a legitimate entity (albeit an international one operating through a proxy). Should an originating telco receive messages using an unregistered sender ID from an international entity, ACCAN considers the originating telco should block the message.

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.

ACCAN considers the proposal is suitable and will incentivise provider participation in the register. As per our response to Questions 18-20, ACCAN considers wide uptake of the register by telecommunication providers is needed to ensure information delivered by SMS is not unnecessarily blocked and the register facilitates positive consumer outcomes.

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?

ACCAN supports over-stamping unregistered sender IDs with 'Likely SCAM'. ACCAN supports the graduated disruption approach and considers the ACMA must conduct a comprehensive assessment of the effectiveness of the register and the over-stamping method 12 months after its implementation.

Question 27: 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 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?

ACCAN supports the proposed reporting obligations. ACCAN considers ACMA must promptly investigate non-compliance by a telecommunications provider or entity of the register and take appropriate action including revoking their approval to participate in the register.

ACCAN notes information sharing requirements will be developed as part of the Scams Prevention Framework and supports the ACMA engaging in regular information sharing with the ACCC and other government agencies to strengthen Australia's coordinated approach to scam prevention.

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?

ACCAN considers the staged implementation is appropriate to ensure providers and customers wishing to use SMS sender IDs are made aware of and comply with their obligations under the Standard. The wide uptake of the register by providers and entities will ensure legitimate communications to consumers are not disrupted. ACCAN supports the ACMA taking a key role in promoting awareness of the register among consumers.

Conclusion

ACCAN thanks ACMA for the opportunity to submit our feedback on the draft Telecommunications (SMS Sender ID Register) Industry Standard 2025. The establishment of a robust and secure SMS sender ID register is a critical step towards achieving positive outcomes for Australian consumers.

The implementation of this register is crucial to its success. Getting it wrong carries significant risks, most notably the erosion of consumer trust in SMS as a communication channel. If the register fails to effectively prevent scams or is perceived as easily circumvented by malicious actors, its impact will be undermined, potentially leading to greater consumer vulnerability and further reluctance to engage with legitimate SMS communications.

Therefore, we urge the ACMA to take a proactive and comprehensive role in the design, implementation, and ongoing management of the SMS sender ID register. This responsibility extends beyond simply establishing the technical infrastructure. It necessitates:

- Rigorous verification processes for participating entities, including the robust framework proposed for international entities through accredited Australian proxy providers.
- Clear and enforceable compliance obligations, with meaningful consequences for non-compliance.
- Effective monitoring and enforcement mechanisms to identify and address misuse promptly.
- Ongoing public awareness campaigns to educate consumers about the register and how it enhances their protection.
- A commitment to continuous improvement based on data analysis, emerging threats, and consumer feedback.

By prioritising security, accountability, and compliance, the ACMA can ensure that the SMS sender ID register delivers positive consumer outcomes and strengthens the digital landscape for all Australians. Should you wish to discuss any of the issues raised in this submission, please do not hesitate to contact Rebekah Palmer, Communications and Policy Officer, at Rebekah.palmer@accan.org.au.

The Australian Communications Consumer Action Network (ACCAN) is Australia's peak communication consumer organisation. The operation of ACCAN is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers. ACCAN is committed to reconciliation that acknowledges Australia's past and values the unique culture and heritage of Aboriginal and Torres Strait Islander peoples.

Advocating for fair communications and digital services

www.accan.org.au
info@accan.org.au