



National Women's
Safety Alliance

AMWA
Australian Multicultural
Women's Alliance

Submission

ACMA Proposed Rules and Operation of SMS Sender ID Register

April 2025

Submitted by

Katherine Berney
Executive Director
National Women's Safety Alliance
www.nwsa.org.au

Malini Raj
Executive Director
Australian Multicultural Women's Alliance
<https://amwa.net.au/>

Acknowledgement of Country

The National Women's Safety Alliance and the Australian Multicultural Women's Alliance acknowledge the Traditional Owners of the land on which we work and live. We pay our respects to Aboriginal and Torres Strait Islander Elders past, present and future. We value Aboriginal and Torres Strait Islander histories, cultures, and knowledge. We extend our respect to Aboriginal and Torres Strait Islander women who for thousands of years have preserved the culture and practices of their communities on country. This land was never surrendered, and we acknowledge that it ***always was and always will be Aboriginal land.***

We acknowledge the strength of Aboriginal and Torres Strait Islander people and communities. We acknowledge that Australian governments have been complicit in the entrenched disadvantage, intergenerational trauma and ongoing institutional racism faced by Aboriginal and Torres Strait Islander people. We recognise that Aboriginal and Torres Strait Islander people must lead the design and delivery of services that affect them for better life outcomes to be achieved.

About NWSA

The Working with Women Alliance (WWWA) represents two key portfolios: National Women's Safety (NWS) and National Women's Equality (NWE). The WWWA connects the critical areas of gender-based violence prevention and the advancement of women's economic equality and leadership, bridging these important policy fields for greater impact.

The **National Women's Safety Alliance** brings together a diversity of voices, expertise, and experience to inform and guide national policy on women's safety. The NWSA, established in August 2021, connects the sector, experts, government, and victim-survivors with a shared vision to end violence against women. This will be achieved through consultation, research, and the collaborative development of expert policy advice to government.

More information about NWSA is available on our [website](#).

About AMWA

The Australian Multicultural Women's Alliance (AMWA) is led by the Federation of Ethnic Communities' Councils of Australia (FECCA), the national peak body representing Australians from culturally and linguistically diverse (CALD) backgrounds in partnership with Settlement Services International (SSI) and Media Diversity Australia (MDA).

The Australian **Multicultural Women's Alliance** is the national voice for multicultural women.¹ AMWA advocates for gender equity, representation, and inclusion across all facets of Australian society. Our work is informed by lived experiences, community insights, and evidence-based research to ensure that systemic barriers are addressed, and opportunities for women are unlocked. As an intersectional alliance, we aim to empower women from all multicultural backgrounds to thrive and contribute fully to Australia's prosperity.

More information about AMWA is available on our [website](#).

¹ When referring to "multicultural" we refer to migrant, refugee, culturally and linguistically diverse (CALD) and racialised women.

Executive Summary

The Australian Communications and Media Authority's *Telecommunications (SMS Sender ID Register) Industry Standard 2025* will protect Australians from SMS scams by censoring SMS messages that use a sender ID.

NWSA and AMWA support the Telecommunications Industry Standard (the Standard) and endorse it as an effective initiative for protecting Australians. While the consultation paper seeks necessary commentary on the model of the Telecommunications Industry Standard, this submission offers a gendered and multicultural lens on the implications of the regulation. NWSA and AMWA recognise that additional cohorts of marginalised women may experience increased vulnerability to scams, but this submission provides insight into how women, and particularly culturally and linguistically diverse women, are affected by scams.

Women experience a far greater risk of victimisation by SMS scams, and this risk is intensified for CALD women. We propose that ACMA frame the Standard as legislation that will progress women's safety, and in addition to the Standard, take measures to address the challenges faced by women, particularly those faced by CALD women, as a result of their increased exposure to SMS scams.

ACMA should also consider how Australia's multicultural population will be affected by the Standard and potential disruption of international SMS, given their ongoing communications with services in their countries of origin.

Key areas for consideration include:

- **Women's Digital Footprints:** Scam prevention is necessarily a gendered issue due to women's higher number of interactions with systems and services, which exposes them to more, and more harmful, SMS scams.
- **Women as Targets of Identity Theft During Experiences of Gender-Based Violence:** The Standard must highlight the intersection between SMS scams and gender-based violence. Experiences of gender-based violence often involve financial and systems abuse that is facilitated by perpetrators gaining sensitive information through SMS scams and proceeding to commit identity theft.
- **Culturally and Linguistically Diverse Women are at Greater Risk of Exposure to SMS Scams:** CALD women are at increased risk of experiencing SMS scams because of vulnerability related to visa status, lack of support networks and social isolation, a limited literacy regarding potential scams, language barriers and a lack of trust in regulatory and complaints systems.

Women's Experiences of SMS Scams

Women's Digital Footprints

Women are overrepresented as recipients of income support payments. They are both beneficiaries themselves, and receive payments as primary carers of others. Women make up approximately 60% of income support payment recipients and receive 70% of carer payments, 90% of parenting-partnered payments, and 94% of parenting-single payments (December 2024).ⁱ Women are more likely to utilise social and health services for themselves and their children. They are almost twice as likely as men to consult a mental health professional, and more likely to consult a GP, dental professional, medical specialist, and to be admitted to hospital.ⁱⁱ

CALD women also interact with both Australian and international systems and service providers at an increased rate, further exposing them to SMS scams impersonating legitimate entities.ⁱⁱⁱ

Whilst it has been established that women are at greater risk of experiencing scams,^{iv} the high prevalence of women engaged in social services suggests two effects that culminate in an increased risk for women, especially CALD women, of SMS scam victimisation:

- *Higher Exposure:* Because women have more communication with sender IDs such as Centrelink, MyGov, NDIS, Health Direct, Capital Pathology, they may have an existing text thread which displays legitimate SMS' from services, and therefore, a predisposed trust in the legitimacy of messages from those sender IDs.
- *More Severe Harms:* As a result of frequent interactions with social services and expansive digital footprints, women are more likely to be compromised during data leaks. They also have more sensitive information stored digitally that can be exploited, resulting in more severe harms.

Women are Targets of Identity Theft as Product of Gender-Based Violence

Two thirds of identity theft cases target women.^v The Australian Competition and Consumer Commission suggest this is an outcome of systemic gender bias: perpetrators may expect women to be easier targets, and can better use their victims' identities due to women often undergoing name changes after marriage or divorce.^{vi} Older victims of bank related identify theft were almost exclusively female.^{vii}

Additionally, women are the primary victims of family and domestic violence and face greater risk of having their partner or ex-partner impersonate their identities to gain sensitive information through services providers, and/or open accounts in their name.^{viii}

Women may experience financial and systems abuse, that includes identity theft, with perpetrators using stolen identities to access bank and credit accounts, or government services in the victim's name. This can have long-term financial and legal consequences for victims.^{ix} The risk of experiencing identify theft, including both financial and systems abuse, is especially high for CALD women.^x

Culturally and Linguistically Diverse Women are at Greater Risk of Scams

Culturally and linguistically diverse people experience both an increased risk of exposure to SMS scams and a heightened vulnerability to harms borne by successful scams. Compounding social and structural factors place CALD women at an even greater risk of scam victimisation.

- *Barriers to Access and Understanding:* Many CALD women experience low systems literacy, particularly around financial and digital systems, and their associated rights and entitlements. Communications from services that regularly use SMS sender IDs (often wrongly) assume background knowledge creating knowledge gaps that can be exploited by perpetrators of identity theft. Additionally, refugees, women on visas, and those with limited English or education face language barriers and social isolation which heighten their susceptibility to SMS scams and identity theft.^{xi}
- *Culturally-Specific Scams and Gender-Based Violence:* Technology-facilitated abuse can include threats uniquely tied to cultural contexts, such as threats of deportation, honour-based violence, or public shaming. Women on temporary or partner visas are especially vulnerable to threats involving their immigration status. Culturally-specific threats are an avenue for perpetrators of scams to intimidate CALD victims to acquire their personal information. Successful identity theft may give rise to perpetrators attempting to sabotage visa applications or threaten deportation.^{xii}
- *Gendered Social Roles:* CALD women, especially refugees, are often highly dependent on partners for finances or access to systems. Exclusion from system-level decision-making and service interactions due to expectations about gender roles make it difficult for women to personally protect their identity and easier for perpetrators to acquire and misuse their identity.^{xiii}
- *Under-Reporting and Distrust in Systems:* CALD women are less likely to report identity theft due to mistrust of authorities, fear of shaming or ostracism within their communities, and concerns about confidentiality. Experiences from their home countries may also make them hesitant to engage with police or government agencies when their identity has been stolen or misused.^{xiv}

- *Higher Financial Losses:* Members of CALD communities report higher average financial losses through scams (\$1,200 compared to \$845 for all Australians).^{xv} This suggests that scams targeting these groups may be more aggressive or exploitative and are more commonly successful.
- *More Systems Interactions and Communications from Sender IDs:* Many CALD individuals maintain ties with institutions in their countries of origin, such as banks, healthcare systems, or social services. With an increased number of text threads with Sender ID's, scammers can exploit reliance on overseas connections by impersonating foreign entities familiar to the victims.^{xvi} This issue is an exaggerated version of the risk associated with women's digital footprints and is especially pertinent for CALD women.

Recommendations

The SMS Sender ID Register is a Women's Safety Initiative

Women are exposed to scams and gender-based violence facilitated by scams at a significantly higher frequency than their male counterparts - the SMS sender ID register will therefore overwhelmingly benefit women. This submission recommends that in developing the Standard, ACMA adopt a peripheral policy framework that acknowledges scam prevention as an inherently gendered issue. A gendered lens must be applied to the Standard, which, if implemented successfully, will contribute to creating safe digital environments for women and restore their autonomy over their sensitive information. Framing the Standard this way will also illuminate the pressing intersections between SMS scams, identity theft, and gender-based violence.

Recommendations

- Framing the SMS sender ID register as a women's safety initiative is an opportunity for ACMA to strengthen their case for the necessity of the regulation, and to acknowledge the role that social and structural factors play in undermining women's safety, particularly in digital spaces.

Data Protection Measures for At-Risk Cohorts

Women from many sub-cohorts have greater systems interactions, and experience higher rates of systems abuse through scams and identity theft. The safety of sensitive information, and the subsequent ability of perpetrators to exploit victims, is dependent on service provider approaches to storing and protecting data.

NWSA and AMWA encourage ACMA to be conscious of the positive correlation that exists between an individual's vulnerability to scams and the degree to which they are involved with systems and services.

Recommendations

- To assist in scam prevention and the implementation of the sender ID register, ACMA must adopt a policy that requires participating entities to have internal protections in place that control the sharing of sensitive information, especially across international borders.
- ACMA should participate in any opportunities or propose their own strategies and industry standards that will help;
 - Limit the circulation of phone numbers leaked through scams,
 - Protect sensitive data by identifying and flagging perpetrators of identity theft, financial abuse, and systems abuse.

- Support victims and targets of scams in setting up account protections and settings that will better safeguard their information.

Multicultural Approach to International SMS Sender ID Messages

CALD individuals often remain reliant on institutions in their countries of origin, such as banks, healthcare systems, or social services. Whilst this provides an additional window of exploitation for scammers, the Standard must appreciate Australia's responsibility for facilitating essential communication between CALD individuals and services in their countries of origin. NWSA and AMWA recommend a tentative and balanced approach to the transit of international SMS sender IDs. ACMA should allow all foreign communications to reach Australian receivers to ensure that no critical communications are terminated. International entities with SMS sender IDs should be required to join the register, and those who do not should have their messages delivered but disrupted with a different over-stamp as a cautionary measure.

Recommendations

- Require foreign entities who wish to use undisrupted sender IDs in communications with Australian numbers to undergo a stringent verification and application process to participate in the sender ID register through an Australian initiating telco proxy.
- Disrupt foreign SMS sender ID messages that are not registered with the Australian standard with a different over-stamp such as 'Foreign Number – Possible Scam.'

Increasing Scam Literacy and Addressing Identity Theft for CALD People

The scale of current interventions to prevent and respond to SMS scams and associated gender-based violence and identity theft is too small relative to the severity and frequency of the incidences faced by CALD women. There is a need for community-led, culturally appropriate and specialised prevention and intervention strategies that ensure CALD women are empowered to protect themselves, and not merely at the mercy of reactive scam prevention campaigns that are inaccessible to them. CALD communities are not homogenous; outreach must be tailored to sub-groups who may be more marginalised or disconnected. One-size-fits-all approaches are ineffective, particularly for identity theft prevention and response, as different sub-groups may face unique risks and barriers to reporting.

Recommendations

- Targeted education campaigns on the prevention of identity theft must be made available in multiple languages and disseminated by trusted community networks

including places of worship, community centres, word of mouth, religious leaders, embassies, and community hubs.

- Existing resources like *The Little Book of Scams* should be translated and converted into multimodal resources such as short translated videos, short sound bites, podcasts and community radio.
- ACMA should approach local multicultural organisations and empower CALD women as leaders and mentors to build trust and improve access to support for identity theft prevention and recovery.
 - Reliance on digital or written communication alone is insufficient given challenges with literacy and distrust of systems. Effective engagement requires targeted, grass roots and face-to-face approaches and ongoing, personalised support.
- Ensure reporting mechanisms and support services are accessible for a diverse number of foreign-language speakers and are designed with appropriate cultural considerations.

ⁱ *Expanded DSS Benefit and Payment Recipient Demographics - December 2024.* (2024). Data.gov.au. <https://data.gov.au/dataset/ds-dga-cff2ae8a-55e4-47db-a66d-e177fe0ac6a0/distribution/dist-dga-38a5c0c7-5246-428b-bc0c-3d1fe153ea78/details?q=centrelink>

ⁱⁱ *Patient Experiences 2023-24 Financial Year.* (2024). Australian Bureau of Statistics. <https://www.abs.gov.au/statistics/health/health-services/patient-experiences/latest-release#data-downloads>

ⁱⁱⁱ *Demystifying CALD: The Complete Guide to CALD Communities.* (2019). All Graduates Interpreting and Translating. <https://allgraduates.com.au/articles/cald/>

^{iv} *Personal Fraud 2023-24 Financial Year.* (2024). Australian Bureau of Statistics. <https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/latest-release>

^v *Identity Theft and Gender.* (2022). Australian Communications Consumer Action Network. https://accan.org.au/files/Grants/ANU%20ID%20theft/ANU%20ID%20theft%20infographic_Gender.pdf

^{vi} *Targeting Scams – Report of the ACCC on Scams Activity 2022.* (2022). Australian Competition and Consumer Commission. <https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf>

^{vii} *Identity Theft and Gender.* (2022). Australian Communications Consumer Action Network. https://accan.org.au/files/Grants/ANU%20ID%20theft/ANU%20ID%20theft%20infographic_Gender.pdf

^{viii} *Targeting Scams – Report of the ACCC on Scams Activity 2022.* (2022). Australian Competition and Consumer Commission. <https://www.accc.gov.au/system/files/Targeting%20scams%202022.pdf>

^{ix} Smith, R. - *Investigating identity crime and misuse in Australia: the role of prevention technologies and the likelihood of victimisation.* (2024). Australian Institute of Criminology. <https://www.emerald.com/insight/content/doi/10.1108/jcrpp-08-2024-0056/full/html> ; Boddy, J., Jianqiang, L. - *Technology-facilitated abuse amongst culturally and linguistically diverse (CALD) women: Service provider's perceptions.* (2023). ANROWS. <https://www.anrows.org.au/project/culturally-and-linguistically-diverse-cald-womens-experiences-of-technology-facilitated-violence-a-mixed-method-study/> ; Zamora, C. et al. - *Technology-Facilitated Abuse Against Women From Culturally and Linguistically Diverse Backgrounds: A Scoping Review.* (2023). Journal of Trauma, Violence & Abuse. <https://journals.sagepub.com/home/tvaa>

^x Boddy, J., Jianqiang, L. - *Technology-facilitated abuse amongst culturally and linguistically diverse (CALD) women: Service provider's perceptions.* (2023). ANROWS. <https://www.anrows.org.au/project/culturally-and-linguistically-diverse-cald-womens-experiences-of-technology-facilitated-violence-a-mixed-method-study/> ; Zamora, C. et al. - *Technology-Facilitated Abuse Against Women From Culturally and Linguistically Diverse Backgrounds: A Scoping Review.* (2023). Journal of Trauma, Violence & Abuse. <https://journals.sagepub.com/home/tvaa>

^{xi} *Hearing her voice: report from the kitchen table conversations with culturally and linguistically diverse women on violence against women and their children.* (2015). Department of Social Services (DSS). <https://plan4womenssafety.dss.gov.au/hearing-her-voice-kitchen-table-conversations-on-violence-against-culturally-and-linguistically-diverse-women-and-their-children/> ; eSafety for Women from Culturally and

Linguistically Diverse Backgrounds. (2019). eSafety Commissioner. [summary-report-for-women-from-cald-backgrounds.pdf](#)

^{xii} *Hearing her voice: report from the kitchen table conversations with culturally and linguistically diverse women on violence against women and their children.* (2015). Department of Social Services (DSS). <https://plan4womenssafety.dss.gov.au/hearing-her-voice-kitchen-table-conversations-on-violence-against-culturally-and-linguistically-diverse-women-and-their-children/> ; Zamora, C. et al. - *Technology-Facilitated Abuse Against Women From Culturally and Linguistically Diverse Backgrounds: A Scoping Review.* (2023). Journal of Trauma, Violence & Abuse. <https://journals.sagepub.com/home/tvaa>

^{xiii} *Hearing her voice: report from the kitchen table conversations with culturally and linguistically diverse women on violence against women and their children.* (2015). Department of Social Services (DSS). <https://plan4womenssafety.dss.gov.au/hearing-her-voice-kitchen-table-conversations-on-violence-against-culturally-and-linguistically-diverse-women-and-their-children/> ; Boddy, J., Jianqiang, L. - *Technology-facilitated abuse amongst culturally and linguistically diverse (CALD) women: Service provider's perceptions.* (2023). ANROWS. <https://www.anrows.org.au/project/culturally-and-linguistically-diverse-cald-womens-experiences-of-technology-facilitated-violence-a-mixed-method-study/>

^{xiv} *Hearing her voice: report from the kitchen table conversations with culturally and linguistically diverse women on violence against women and their children.* (2015). Department of Social Services (DSS). <https://plan4womenssafety.dss.gov.au/hearing-her-voice-kitchen-table-conversations-on-violence-against-culturally-and-linguistically-diverse-women-and-their-children/> ; Boddy, J., Jianqiang, L. - *Technology-facilitated abuse amongst culturally and linguistically diverse (CALD) women: Service provider's perceptions.* (2023). ANROWS. <https://www.anrows.org.au/project/culturally-and-linguistically-diverse-cald-womens-experiences-of-technology-facilitated-violence-a-mixed-method-study/> ; Zamora, C. et al. - *Technology-Facilitated Abuse Against Women From Culturally and Linguistically Diverse Backgrounds: A Scoping Review.* (2023). Journal of Trauma, Violence & Abuse. <https://journals.sagepub.com/home/tvaa> ; eSafety for Women from Culturally and Linguistically Diverse Backgrounds. (2019). eSafety Commissioner. [summary-report-for-women-from-cald-backgrounds.pdf](#)

^{xv} *Scam Losses to Culturally Diverse Communities', People with Disability and Indigenous Australians Almost Doubled in 2021.* (2022). Australian Competition & Consumer Commission. <https://www.accc.gov.au/media-release/scam-losses-to-culturally-diverse-communities-people-with-disability-and-indigenous-australians-almost-doubled-in-2021> ; *Scammers Increasingly Targeting CALD Communities.* (2022). AMES News. <https://amesnews.com.au/latest-articles/scammers-increasingly-targeting-cald-communities/>

^{xvi} *Culturally and Linguistically Diverse Community Lose \$22 Million to Scams in 2020, Reports from Indigenous Australians up 25%.* (2021). Australian Competition and Consumer Commission. <https://www.accc.gov.au/media-release/culturally-and-linguistically-diverse-community-lose-22-million-to-scams-in-2020-reports-from-indigenous-australians-up-by-25-per-cent> ; *Scammers Increasingly Targeting CALD Communities.* (2022). AMES News. <https://amesnews.com.au/latest-articles/scammers-increasingly-targeting-cald-communities/>