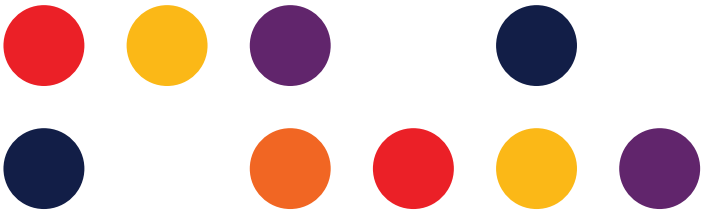
Fighting SMS Scams – What type of SMS sender ID registry should be introduced in Australia?

TPG Telecom submission

Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA)

March 20, 2024

[redacted]



Submission

Thank you for the opportunity to provide a submission in response to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) consultation into the proposed status of an SMS Sender ID Registry (**the Registry**).

TPG Telecom also contributed to the submission by Communications Alliance.

About TPG Telecom

TPG Telecom is Australia's third-largest telecommunications provider and home to some of Australia's most-loved brands including Vodafone, TPG, iiNet, AAPT, Internode, Lebara and felix.

We own and operate nationwide mobile and fixed networks that are connecting Australia for the better.

We are an active member of the Australian Communications and Media Authority (ACMA) voluntary pilot for the Registry.

We established and continue to run the first cross industry led operational anti-scam task force sharing operational information with other telecommunications service providers, finance institutions, government bodies and law enforcement agencies.

Executive summary

TPG Telecom supports Option 2, a mandatory Sender ID registry acting as an 'allow-list' for alpha-tagged SMS. Scam Short Messages (SMs) should be prevented from being allowed to be sent in the first place - particularly in the form of alphanumeric Sender ID SMs, which appear to victims as legitimate communication from a trusted organisation.

Without a defined, mandatory model, the general public will remain unable to trust SMS sent by businesses and government services.

Only by developing a mandatory, trusted, closed ecosystem for sending alphanumeric Sender ID SMs will the public, businesses, and the telecommunication industry see a reduction in scam communications, to enable the telecommunication industry deliver the expected security of SMS communications. In such an environment a clear message can be given to the community that alpha-numeric Sender IDs can be trusted.

A voluntary 'block-list' scheme would leave the door open for bad actors to continue to send scam SMs by overstamping, mirroring or impersonating legitimate Sender IDs as they are today – voluntary scheme lists have infinite options available for impersonation.

All alphanumeric Sender IDs must be registered prior to use and whitelisted as valid traffic. All other alpha-numeric Sender ID traffic must be blocked. This is the only way to establish a trusted ecosystem for alpha-tagged SMs free from scams.

The registration of an alphanumeric Sender ID should not restrict the use of that Sender ID to one user. Multiple brands could register the same Sender ID, provided they can demonstrate a connection to the Sender ID. Any decision to grant a Sender ID should be reversible if authentication was incorrectly granted or information was incorrectly broadcast to the aggregators participating in the

scheme.

Opponents of a mandatory scheme do so on the basis that the registration process would be too difficult and onerous. While this may be true for some overseas models it does have to be the case of an Australian model and the perceived difficulty of mandatory registration needs to be balanced against the real cost to the community of enabling SMS scams to flourish.

Responses to consultation questions

1) *Have you, your organisation, or clients been targeted by SMS impersonation scams that used your alphanumeric sender ID(s)?*

Yes.

2) *Do you support the introduction of a voluntary or mandatory SMS Sender ID Registry for alphanumeric sender IDs? Why?*

We support Option 2, a Sender ID registry as a mandatory 'allow-list' for alpha-tagged SMS. A trusted, alpha-tagged SMS ecosystem will enable businesses and government services to communicate with the public in a safe, secure, and accessible way by SMS.

Any other register scheme would be reactionary, would not block all scam traffic, and would be unwieldy to manage while failing to protect the public and businesses from SMS impersonation scams.

While the cost of scams to the public is widely reported, there is also a cost to businesses and government services in the loss of trust in using SMS as a tool to connect. The ACMA's own research in the 'How we Communicate' report shows that 91% of Australians use SMS as a method of communication in 2022. The opportunity cost of avoiding this simple and easily available method of communication has not accurately been measured. However, the impact is growing as more people become aware of the risks and associated scams.

Under a voluntary scheme, pathways would remain available to bad actors to send alpha-tagged SMS. [redacted]. Industry can attempt to block many variants of the real Sender ID, but the problem is endless. Fraudsters will find the next best ID to deliver scams. A case study based on a recent scam event has been provided in **Appendix A**. [redacted]

We have previously sought to demonstrate the complexity to the public of identifying scams in our 'Spot the Scam' presentation, provided in **Appendix B**.

The Registry

To address this risk, a mandatory Registry body must provide an easily accessible model (e.g. a specific webpage). It must be empowered to approve or decline an applicant's requested alphanumeric Sender IDs based on validation of the data provided using digital identity solutions (e.g. MyGov). Please see **Appendix C** for an example of a proposed Registry model.

The Registry body should require trading names, company names or reasonable grounds for using each Sender ID requested, including the following:

- Requested alphanumeric Sender ID;
- Associated brand;
- Ownership details of that brand to enable a check against relevant registers (e.g. ASIC, ACNC, Company Name, ABN, ACN);
- Authorised contact details (Contact Name, Contact Phone Number, Contact Email Address);
- Digital identity

- Proposed SMS aggregator(s); and
- Technical details (TBC).

The Registry should also have the capacity to allow SMS aggregators to validate that a Sender ID is assigned to a requesting party.

Validation and authentication can be best achieved via an API or registration token from the Registry to enable automation within the ecosystem. Once validated, the SMS aggregators would commence the requested campaigns with receiving telcos accepting all traffic containing the registered, confirmed Sender IDs.

The registration of an alphanumeric Sender ID should be for a set period (e.g. 5 years), with the registered brand confirming an ongoing connection to the tag to avoid the registration expiring. This will prevent the potential misuse of old or unused tags.

The Singapore model

While TPG Telecom has not been involved in the Singapore model, at a general level, we do not support the limitation of Sender IDs to the first registered party or the use of the 'likely scam' overstamp. Any mandatory Australian solution must allow multiple businesses that have been appropriately authenticated as having a valid case for using a specific alphanumeric Sender ID to continue to utilise the same alphanumeric Sender ID (as is the case today). For example, the Australian Bureau of Statistics and American Beauty Supplies could both register and use the Sender ID 'ABS' to send SMS. Note: The message content gives context to the source and relevance to the party receiving the message through the information contained in the message.

Cost

Funding for the Registry should be sourced from general revenue.

The one exception would be to support the operation of specific functions where there is a direct benefit to be derived from its activities, such as a fee or charge for business registration of an alphanumeric Sender ID (similar to the annual cost of dedicated marketing numbers such as 13 TAXI). This charge should only cover the scheme's administration cost (i.e., not a for-profit).

3) What, if any, transition arrangements are required?

We recommend further discussion and consultation on operationalising a mandatory Register.

[redacted]

Appendix A: Case study

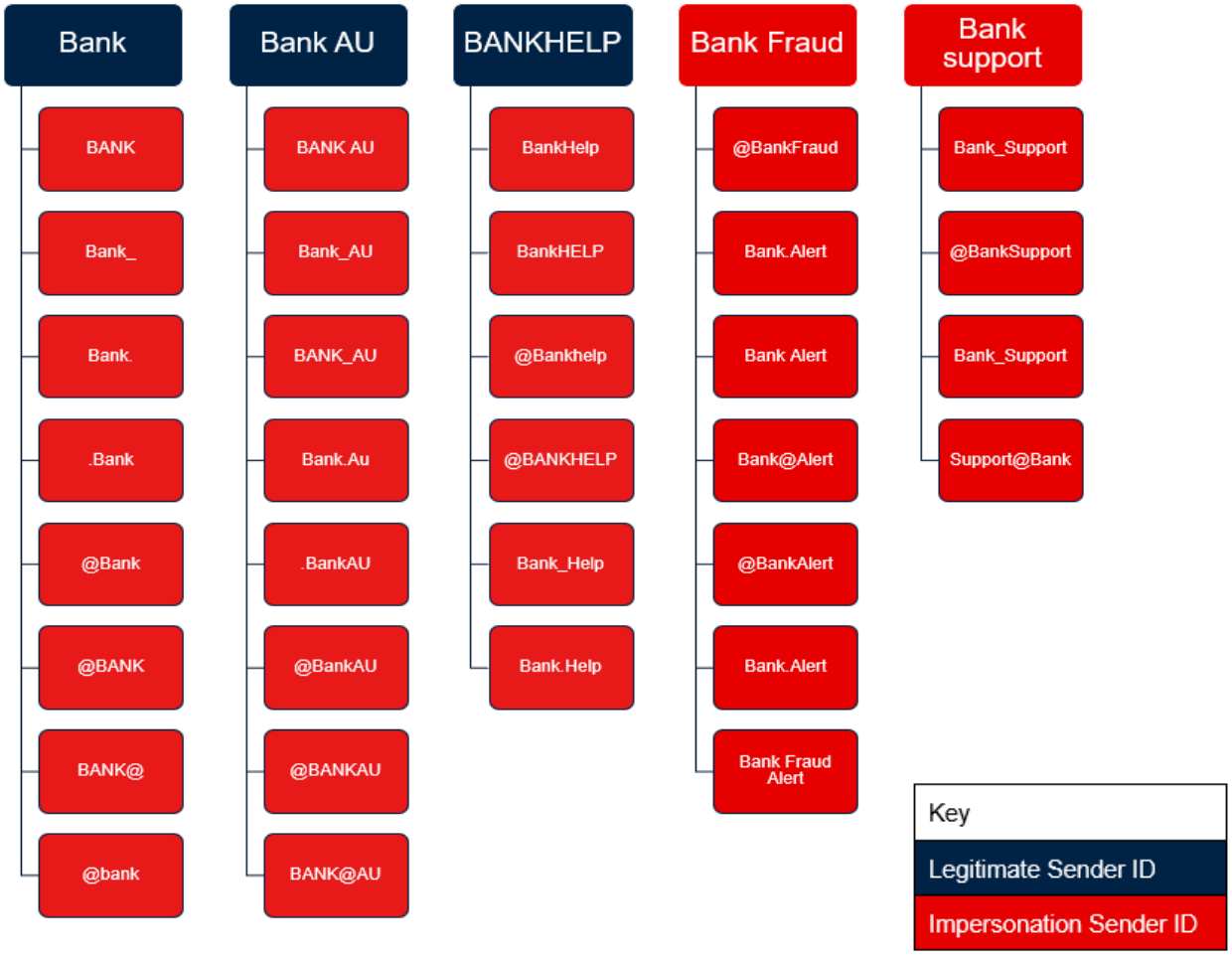
(Note – this case study is based on a current scam campaign. The specific Sender ID's have been de-identified; the material issues have been retained.)

[redacted] It has 3 legitimate Sender IDs:

(1) Bank
(2) Bank AU
(3) BANKHELP

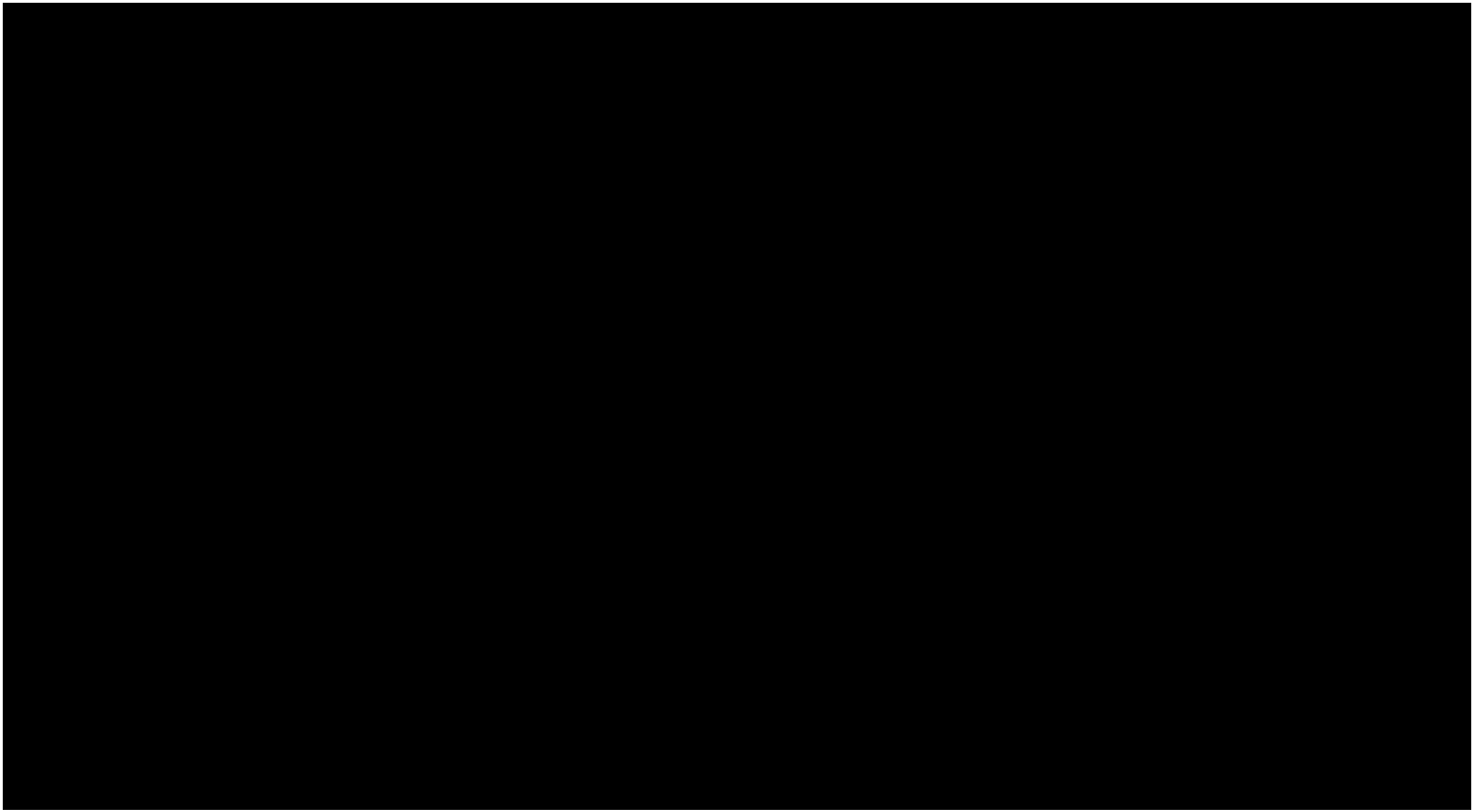
Sender ID impersonation began on Sender ID (1). First, it was impersonated by changing the case (BANK). Once this was identified and blocked, fraudsters began adding punctuation to bypass filters (Bank., Bank_, @BANK). Once common punctuation was added to SMS firewalls, fraudsters moved to the next legitimate Sender IDs and began the process again. They also created impersonation Sender IDs that would easily be assumed by customers to be legitimate (Bank Alert, Bank Fraud Alert, Bank Support). Once these were blocked, they started the process of creating alternatives through case sensitivity and punctuation.

This is an ongoing campaign. It is expected that fraudsters will simply move to another unprotected and untapped brand once this campaign is over. It is not possible to guess or guarantee where the attention will shift to.



Appendix B: Spot the Scam

[redacted]



Appendix C: Registration model