10 March 2023

Ms Silvia Superina
Manager, Strategy and Projects
Australian Communications and Media Authority
ACMA file reference: ACMA2023/95-2

By email: senderIDregistry@acma.gov.au

Dear Ms Superina

**Options for an Australian SMS sender ID registry**

COBA appreciates the opportunity to contribute to the Government's consultation on options for an Australian SMS sender ID registry.

COBA is the industry association for Australia's customer owned banks (mutual banks, credit unions and building societies). COBA members are an important part of Australia's payments system, providing a wide range of payment products and services to 5 million customers. Collectively, our sector has over $160 billion in assets and is the fifth largest holder of household deposits. Customer owned banks account for around three quarters of the total number of domestic Authorised Deposit-taking Institutions (ADIs) and deliver competition and market leading levels of customer satisfaction in the retail banking market.

**Key points**

COBA strongly supports the introduction of an SMS register to reduce scam texts and impersonation of trusted brands

ACMA is encouraged to adopt the National Anti-Scam Centre (NASC) development principles to 'integrate and not duplicate' existing frameworks and bodies.

Timelines and costs should not create barriers for customer-owned banks to protect their customers from scams originating from SMS channels.

Once key priority trusted sectors such as banking and government are in the register, criminals will use other sectors, so the register needs to be able to expand to adopt an Australia wide approach.

COBA strongly supports the introduction of an SMS register to block and track scammers who are impersonating customer owned banks and causing harm to Australians. We see the introduction of a Australian SMS registry as being key to closing the gap on SMS scams as this crime wave moves from country to country. Customer owned banks need to be able to rely on "authorised and locked in "Alphanumeric tags" to stop criminals manipulating customers and using brand trust to cause financial harm. We support a model where participation is mandated as the strongest possible means to safeguard consumers against potential scams as well as facilitate tracking when scam messages were sent to local mobile users.

COBA offers in principle support for **Model 2** as detailed in correspondence. We note this requires all alphanumeric sender IDs to be registered and blocks all unregistered IDs. We note this model is currently being implemented in phases in Singapore. We further understand that based on industry discussions this model is preferred noting Singapore considered the UK model combination approach and rejected it in favour of simplified whitelist.

COBA supports a model where all participants are registered, and aggregators licensed and subject to penalties if they fail to comply with regulations that govern SMS registering.

COBA notes that the new mandatory Singapore SMS Sender ID Registry ("**SSIR**") regime is part of an ongoing multi-layered approach to strengthen protection against scams. We note the strong results from the phased model adopted in Singapore who report a 64% reduction in scams through SMS. COBA also acknowledges the results achieved by Telcos to reduce scam calls and SMS that have resulted in 90 million scam SMS blocked since July 2022 and 955 million scam calls blocked since December 2020.

To address the specific responses to questions posed in ACMA **Attachment A: Sender ID registry targeted consult**, we have attached a document combining responses from a representative sample of sector members large and small. In addition, we have included points for consideration relative to the broader risk that SMS brand impersonation presents to all Australian business that utilise SMS as trusted means of interacting with their customers.

### Integrative principles (National Anti-Scam Centre)

ACMA is encouraged to adopt the National Anti-Scam Centre (NASC) development principles to 'integrate and not duplicate' existing frameworks and bodies. As criminals move to exploit gaps here and in other counties who have adopted or implemented an SMS registry, we recommend that consideration be given to how information is collected, shared, stored, and used by relevant parties to disrupt scam activities. In this case telecommunications providers will have access details used to impersonate genuine businesses which law enforcement will need to access for prosecution and disruption.

### Barriers to participation (Timeline and Cost)

Customer owned banks scale and size along with dependence on third party providers can mean there is a longer lead time needed to participate and build in compliance measures. COBA members provide much needed competition in the banking market, and most rely on outsourcing to obtain efficiencies and economies of scale.

Costs are also a barrier to participation, in respect of both these points we ask the ACMA consider the design of simple sign-up processes including authorisation. We note the cost to list to the Singapore registry is not dissimilar to costs to register and hold a 1300 or smart number. We support the most economical method and note we would expect registration costs to be self-funding (on scale) per number.

### Targeting industry as an ecosystem (Adopting an Australia wide approach)

To ensure the integrity of process we believe that there will need to be cross validation with other regulators/third party vetting required. Once banks and other Government departments move to register details the risk of transfer to other less mature industries will take place. This could see data being harvested through criminals targeted retailers and smaller service providers.

We look forward to engaging with the ACMA on this issue and thank you for taking our views into account. Please do not hesitate to contact Leanne Vale, Director Financial Crimes and Cyber Resilience lvale@coba.asn.au if you have any questions about our submission.

Yours sincerely,

**MICHAEL LAWRENCE**
**Chief Executive Officer**

**Sender ID registry targeted consult – CUSTOMER OWNED BANKING ASSOCIATION – COLLATED FEEDBACK.**

**Not for public release**

| Questions |
|---|
| **Support** |
| *Do you support the introduction of a Sender ID registry? Why/why not?* <br><br> Yes.  COBA members support the introduction of a Sender ID registry. It is primarily supported it in light of recent events of customer fraud due to malicious actors mimicking sector sender IDs. It is also supported as a means of reducing emotional and financial harm to receivers of SMS and those who rely on trusted messaging for business. |
| **Model** |
| *Do you have views on a potential model? Should a model permit voluntary registration of alphanumeric sender IDs OR require all IDs to be registered?* <br><br> COBA members support the concept of **model 2 in** the ACMA feedback letter, which is the introduction of a mandatory registration of all Sender IDs. This should be mandatory rather than voluntary for Telcos and participants |
| *In addition to SMS sender IDs, should a registry also allow trusted brands to register phone numbers used to send SMS messages to customers?* <br><br> COBA members support the concept of a registry that incorporates registration of dedicated mobile numbers used by trusted organisations.  Additionally strong governance is required for registration to stop criminals registering similar brand names |
| **Delivery** |
| *Who should operate and administer a registry? Government, industry or outsourced? Why?* <br><br> COBA members support either Government or industry administration. However, if it is outsourced to industry that it should be covered by adequate compliance and regulation to ensure that the scheme is effective, well monitored and enforceable. |
| *By what mechanisms should registry details be provided to telcos?* <br><br> COBA members support any registry solution being dynamic and real-time rather than reactive and manually maintained. Secure two way entry exit and integration with existing systems so that there is minimal gap time |
| *Are there specific security concerns or recommendations that should be considered for a registry?* <br><br> COBA members support the introduction of a registry that should accommodate registration for legitimate sender IDs that originate from outside Australia and that are sent on behalf of the trusted brands by authorised industry partners. This is predicated on the above point, that the solution be dynamic and real-time. |
| *Would you support interim or staged implementation if it means consumer safeguards are in place sooner?* <br><br> COBA members support initiatives that are workable across the industry if that helps alleviate instances of customer fraud through SMS. We have no preferred implementation approach.  Given the upward trajectory of scams through  SMS and impact on customer trust there is merit in this being a sooner rather than later approach. |
| **Benefits and impacts** |
| *What would be the benefits, including financial and social?* <br><br> COBA members believe that there would be both financial and social benefits with the introduction of an SMS registry, including but not limited to maintaining the reputation of trusted brands. A failure to act will lead to reduced trust in the financial system and an overall reduction in the ability to protect the financial safety of the Australian community. |
| *Other than any potential fees for using the registry, what impacts, including costs, may be involved for your organisation? Please provide detail.* <br><br> In the event that a COBA member is currently using a SMS gateway provider that does not correctly implement a compliant registration system, some COBA members may need to consider changing service providers to protect our customers with the integration and contract expenses that this entails. This may add additional development efforts and time/ costs. COBA members support a simple easy to use model that is similar to registering and paying for 1300 numbers <br><br> COBA members support a self-registration process but through only trusted licenced proven entities otherwise criminals will simply move into this space and create fake registrations. All telcos must be regulated in  way that ensures active participation if they provide the service or number/alpha tag. |

*Are there potential impediments to consider?*

Any registration system should consider the ability to have more than one SMS gateway provider share the same authorised sender ID to provide SMS service provider diversity for the trusted brand.

*Should compliance with the registry be enforceable (by a regulator)?*

Yes. COBA members absolutely support an enforceable compliance regime that is administered in a way to similar to how ACMA and the Communications Alliance is currently managed. COBA members support fines for noncompliance as currently exist.

*How could a funding model work if a registry operated on a cost neutral basis to govt? Should brands, telcos or both meet any costs?*

COBA members support a modest cost recovery model by the trusted brands. This is also to consider that Telcos and aggregators are in essence selling a service that is being used for criminal activity

*If a registry is in place, where should consumers complain if they receive SMS scams using registered alphanumeric Sender IDs?*

COBA members would envisage that ACMA be the entity that handles consumer complaints as a result of SMS scams.

**Scam disruption**

*What has been your/parent company's experience using any O/S model or provider-level registry?*

Some COBA members have been impacted by the introduction of the mandatory Singapore registration model, in that the process is onerous when viewed against the number of SMS that COBA members do send to Singapore-based numbers. In particular, the requirement to register a Singapore-based entity.

*What strategies do you currently use to combat brand impersonation in SMS? How could a Sender ID registry enhance or complement them?*

COBA members undertake regular and ongoing customer education messaging through platforms such as Social Media. In addition, and also add reminders contained in most SMS to not share One Time Passwords with anyone else, including the bank. Scam alerts are placed on social media and as an online banner on some COBA members digital banking apps and online banking.

**Other**

*How many different alphanumeric sender IDs do you currently use to send text messages to your customers?*

For example, a large currently has approximately 8 senders IDs, including those sent by authorised industry partners. A smaller COBA member has 6 sender ID's, with **5-8 being average**
COBA members also rely on third party aggregators to send SMS to validate transactions and believe regulation is needed to ensure all participants who send SMS are registered.

*Are there other matters that may assist the ACMA to provide advice on the implementation of a Sender ID registry in Australia? Please provide detail.*
COBA members believe that layers of Telco resellers must be easily identifiable and available to end users of which the downstream experience has been frustrating and taken months to get an answer back that the middle Telco wont act or refuses to acknowledge a request for DNO or SMS protection of Alpha tag.

COBA members support :
1.  A technical solution to be put in place to prevent SMS fraud from originating outside of Australia; and
2.  Participants within trusted sender ID brands having access to a portal where they can manage their own sender IDs and SMS gateway providers.

**Other Comments**
The registry must compel all smaller Telcos and aggregators including bulk service providers to register all senders, the situation that exists with smaller Telcos and Do Not originate is an example of why an all in approach must be taken .
High risk transactions being authenticated by SMS is subject to protections by trusted source providers now such as customer owned banks but in this instance, we are unable to control origination which is at the channel being the Telco.

COBA members report (At least six organisations) having spent months waiting for responses from Telcos, where they have acted as instructed and referred to Account Managers and relevant senior staff with requests to protect Trusted Source Alpha tag and via process of Do not Originate, Do not Authenticate and Do Not Terminate Limited success and fractured responses have contributed to the harm these scams are causing. The registry is a step towards removing barriers but must be all Telcos and adopted by all Australian businesses to be effective and build scam resilience.