Australian Banking Association

Submission: Fighting SMS Scams Consultation Paper

25 March 2024

Australian Banking Association

Table of Contents

Australian Banking Association

Key Recommendations

The Australian Banking Association (ABA) welcomes the Australian Government's actions across all parts of the scams ecosystem to prevent and respond to scams affecting Australians. The proposed SMS Sender ID Registry would help to protect Australians from spoofed sender IDs, that is, where scammers hide the number that they use to send an SMS with an alpha-numeric tag used by or associated with a legitimate organisation or brand, for example, 'MyGov'.

ABA strongly supports making the proposed SMS Sender ID registry mandatory, as this would provide greater coverage, confidence and security, for legitimate organisations and their customers. After Singapore implemented a mandatory SMS Sender ID Registry in March 2022, there was a 64% reduction in scams through SMS from Q4 2021 to Q2 2022.[1]

A mandatory registry would:

- ensure only registered sender IDs can be used;
- give consumers greater clarity about whether they can trust SMS communications; and
- protect organisations that use two or more carriers (for operational resilience or other reasons) to send SMSs from the same sender ID.

ABA provides detailed comments and questions about the proposed registry in the next section.

ABA members have been working on initiatives with telcos and also calls on the Government and the telecommunications sector to undertake further initiatives that would hinder scammers' ability to use other forms of telecommunications to contact and socially engineer Australians. Collectively, these additional initiatives would create a more comprehensive impediment to scams than a SMS ID Registry alone.

In addition to spoofed sender IDs, scammers use a range of other means to contact potential victims using telecommunications networks. ABA calls for action to address these avenues for scam communications, otherwise, there is a real and significant risk scammers would migrate to these other avenues once an SMS sender ID registry is established. For example:

- protecting other types of SMS, such as two-way SMS;
- protect against spoofing scam calls: scammers can spoof legitimate phone numbers when scammers make outbound calls to customers;
- information sharing and acting on intel: where a bank or another trusted party reports a scam SMS or phone call, or a scam phone number or URL in a scam SMS), carriers should take prompt action;

[1] Infocomm Media Development Authority, 'Anti-Scam Measures': https://www.imda.gov.sg/how-we-can-help/anti-scam-measures

- notification for affected brands: consider whether telcos could notify organisations where their brand has been impersonated for scam purposes. This may be useful where the telco that identifies the scam does not originate the call or SMS.

Policy Director contact: [redacted]

Policy director

About the ABA

The Australian Banking Association advocates for a strong, competitive and innovative banking industry that delivers excellent and equitable outcomes for customers. We promote and encourage policies that improve banking services for all Australians, through advocacy, research, policy expertise and thought leadership.

Australian Banking Association

Detailed Submission

Introduction

Methods used by the criminals to make initial contact with and socially engineer Australians are Australia's first line of defence in fighting scams. The main 'sources of scams' in Australia are SMS, phone calls, digital platforms, and email.

According to the National Anti-Scams Centre's second quarterly update, text messages were the most frequently used method of contact, accounting for 38% of all scam contacts reported to ScamWatch over October-December 2023). Phone calls were the third most frequently used method of contact at 17% of contacts.

A key enabler of many scams is the ability for scammers to impersonate a different identity, including the brand of trusted organisations, companies, or government. In addition to the harms that are experienced by scam victims, such impersonation also undermines consumers' trust in digital communications and digital interactions.

Measures that would make it more difficult for scammers to assume a trusted identity (such as by impersonating a brand) when contacting Australians, or to block such impersonation communications outright, are a critical component of Australia's overall approach to tackle the scourge of scams.

Whether the proposed registry should be mandatory

ABA strongly supports the proposed SMS ID registry being mandatory.

- A mandatory registry will require all carriers and all brands that use sender ID in Australia to participate, thus creating a 'white list'. This is likely to be more effective at preventing brand impersonation than a voluntary registry which would use a block list or black list. Specifically, ABA understands and seeks confirmation that a mandatory registry would require all carriers to block the use of registered Sender IDs (or alpha tags) from unauthorised sources, no matter which network the alpha tag is attached to.
    - A white list approach means that only registered SMS sender IDs can be used. This gives organisations greater confidence in protecting their brand, and gives users greater confidence in the legitimacy of an SMS from a business.
    - By contrast, a black list approach would require legitimate organisations to black list multiple potential alternatives of their organisation's sender ID. It is likely necessarily incomplete or subject to gaming by scammers, since recent enforcement outcomes suggest carriers face difficulties determining whether a sender is entitled to use a sender ID;
- A voluntary registry could give consumers false confidence in SMS sent with a sender ID. Alternately it can create confusion as to which sender IDs can be trusted, which may undermine consumer confidence in SMS communication;
- ABA understands that a mandatory registry can provide protection for SMS sender IDs where two or more carriers are used to originate SMSs from a sender ID, but this

arrangement is not protected by a voluntary registry. A brand may use multiple carriers for a range of reasons including operational resilience and cost;

- A mandatory registry would broaden the user base for the registry and thereby lower the cost of registration for all users. Also refer ABA's comments below on who should bear the costs of operating the registry.

Impact on related proposals

The ACCC recently consulted on a draft report as part of its inquiry into domestic transmission capacity service, fixed line services and domestic mobile terminating access service.[2] One of the proposals put forward in the draft report is to regulate application-to-person (A2P) SMS termination services (i.e. bulk SMS). Some submissions to the consultation raised a concern about whether regulating access to SMS termination services can result in an increase in scams, because telcos would lose the ability to block SMS coming from these services.

ABA considers that, if this proposal is adopted and this increases the risk of scams being conducted using bulk SMS, it will be necessary to adopt a mandatory SMS sender ID registry and potentially other measures to mitigate the increased risk.

Operations and cost of the proposed registry

Operations of the registry

ABA seeks consideration and clarification on the operations of the registry:

- Process for registering a sender ID, especially given potential volume at commencement.

- Preceding launch of the register, effective communications and awareness for all brands that may use the registry. Likewise, a broad-based and robust awareness campaign will be necessary to ensure consumers understand any changes they may see in the SMSs received, how to assess any warnings they may receive and where to go for further information or guidance.

- What happens when an SMS sender ID is not registered:

    - Consider if it is appropriate for all messages sent with unverified Sender IDs to be blocked, or whether different controls may be applied. For example, consider numbers associated with Government entities.

    - If not wholly blocked, consider how to present warnings or alerts about unregistered IDs (ie, 'unverified sender'), if these SMSs will not be wholly blocked. This will need to be supported by a robust public education campaign so the public understands what the warning means.

[2] ACCC, *Public inquiry into the declaration of the domestic transmission capacity service, fixed line services and domestic mobile terminating access service, Draft report* (December 2023), at: https://www.accc.gov.au/by-industry/regulated-infrastructure/regulatory-projects/public-inquiry-into-the-declaration-of-the-domestic-transmission-capacity-service-fixed-line-services-and-domestic-mobile-terminating-access-service/draft-report

  - If wholly blocked, would the sender be notified that it has been blocked and can the sender resend the message without the alphatag.

  - Establishing a process for telcos that have blocked a SMS to inform the brand that has been impersonated, so the brand can investigate and take any further action necessary to protect their brand.

- Ensuring the legitimacy of the organisation registering a sender ID:

  - Is it intended that the registration would be set up similar to trademark registration? (e.g. registered name for certain good/services/industries)

  - Would there be a window for persons to object to a registration such as there is for trademarks?

  - Will every organisation need to have a completely unique sender ID, if so will there be rules around how similar IDs can be?

- ABA highlights the following considerations about Singapore's SMS ID registry:

  - Singapore's registry does not appear to include a mechanism for third parties to dispute a registration. This could potentially facilitate ID squatting. ABA acknowledges that Singapore's registry requires supporting documents if the proposed Sender ID is not clearly linked to the company or business name, and generic IDs are not permitted.

  - Singapore's registry does not allow more than 1 business to use the same Sender ID. However, there is a mechanism to allow representatives to use a Sender ID on a business' behalf (e.g. a marketing firm engaged by the business). It would be worth exploring if companies within the same corporate group could register to use the same Sender ID and additionally have an authorisation mechanism.

  - ABA understands that Singapore's ID registry blocks SMSs sent with an unregistered ID. In the initial phase, Singapore's registry labelled unregistered IDs as 'potential scam'. Refer to questions above about the operations of the registry.

  - Consideration also needs to be given to if/how foreign entities can register. For example, in Singapore, foreign entities can register for a 'unique entity number' that would then allow them to register their Sender ID.

Cost of participation

ABA does not agree with the proposal that the cost of operating the proposed registry should be entirely borne by businesses registering. ABA considers carriers should bear some share of the cost, as is the case for a number of banking industry anti-scams initiatives.

Carriers have regulatory obligations to ensure that scams are not enabled through their platforms, for example, to ensure their customer has a right to use the phone number. ABA considers a

proposed registry can be seen as a reasonable business cost to meet these obligations. Further, given telcos are currently required to undertake checks to ensure the legitimate use of sender IDs, it is likely that a mandatory register would reduce the costs and regulatory burden associated with ensuring sender ID use legitimacy.

ABA draws a comparison to the banking industry's initiative to build an industry-wide Confirmation of Payee service at a cost of $100 million, as part of the ABA and Customer-Owned Banking Association (COBA)'s Scam-Safe Accord. The investment in this service is being funded by banks.

Transition

ABA supports the Government's and ACMA's current approach of establishing a voluntary registry while work is underway on a longer term, mandatory registry.

ABA supports a reasonable transition period for establishing a registry under legislation, and considers 6 months a reasonable transition period.

Further initiatives

The proposed SMS Sender ID Registry will be a significant capability to protect Australians from scams, however, scammers will evolve and respond by migrating to other contact methods including other ways of contacting customers by phone, SMS, social media and other digital platforms. A more comprehensive approach is required to hinder scammers' ability to use telecommunications to perpetrate scams at scale.

For this reason, the ABA asks the Government and the telco industry to consider adding these capabilities to the telecommunications arrangements in Australia, either via the proposed SMS Sender ID Registry or other initiatives.

- Protecting other SMSs, including two-way SMS (for example, an SMS notification to a customer that requires the customer to respond to say whether the transaction was authorised or not) and SMS sent with a number not sender ID.

  ABA understands that, currently, two-way SMS cannot be sent with an alpha-tag, but are sent with regular mobile numbers. If this is the case, ABA asks the Government to consider how these types of SMS can also be protected. Secondly, scammers can send SMS without a sender ID which can still impersonate organisations.

- Preventing spoofed phone calls: ABA also calls for the introduction of measures to protect phone numbers used on phone calls, in addition to protecting SMS.

  Scammers can spoof numbers on phone calls. Scammers can hide their number and replace (for example) an overseas number with an Australian number and/or with the number of a recognised organisation. This allows the scammer to impersonate an organisation or brand via phone calls, and also increase the chances of a customer answering a call and trusting the scammer.

  Over the period of October-December 2023, based on consumer reports to ScamWatch, phone calls were the third most used contact method at 17% of reported cases, and is the contact method that results in the highest losses at $24.5 million. The telecommunications industry's Do Not Originate register protects Inbound calls but can be difficult for some

organisations to access. The ABA asks for the accessibility of the Do Not Originate register to be enhanced and for the DNO register to expand its capability to protect Outbound numbers.

- Establish a robust takedown mechanism that applies to telcos, as well as other platforms or companies that form the key sources of scams. When a trusted party (such as a bank or the NASC) reports a scam SMS or phone number, the recipient entity should be required to investigate promptly and take down, block or otherwise take action on a confirmed scam.

  The information sharing trial conducted by Optus and the major banks has demonstrated this concept can be applied in practice, and can be applied to protect phone calls and other forms of SMS that do not use alpha tags.

  This proposal can be implemented more broadly by building on and bringing together proposed mandatory scams industry code obligations concerning information sharing, reporting, responding to and taking down scam content, and record keeping.

- Notification of affected brands: as set out on page 6, having a process for telcos that identify a scam SMS or phone call to notify the affected brand. This may be useful where the telco that identifies the scam does not originate the call or SMS. ABA highlights the banking industry is working with the Australian Financial Crimes Exchange to productionise an intel-reporting and notification capability, with a number of carriers having participated in a trial that commenced in July 2023.