Commonwealth Bank

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

Response to Consultation Paper

20 March 2024

Public

1. Introduction

The Commonwealth Bank of Australia (CBA) welcomes the opportunity to respond to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts' (the Department) Consultation Paper, *Fighting SMS Scams – What type of SMS sender ID registry should be introduced in Australia,* released in February 2024.

CBA supports the introduction of the SMS sender ID Registry (the Registry), which will play an important role in combatting scammers and minimising the methods by which they can contact and deceive consumers. Scammers typically deceive consumers by using a combination of services; however, telecommunications channels, in particular text messages, are a preferred method.

The National Anti-Scam Centre's (NASC) scam statistics highlight that, of all scams reported in 2023:

- there were 108,636 reports of phishing scams, representing 36 per cent of all scam types;
- text messages were the most common delivery method across all scam types (comprising 36 per cent). For phishing scams, texts were the delivery method in 51 per cent; and
- phone calls accounted for the highest losses at $116 million (or 24 per cent of reported losses).[1]

We note these figures are likely to be considerably underestimated given they rely largely on consumers self-reporting.

CBA continues to deliver initiatives to help protect customers from scams and we are also collaborating with telecommunications providers on new ways to help detect scammers. Some of these initiatives include:

- CallerCheck – verification of calls from CommBank via the CommBank app, with 2 million calls verified;[2]
- Scam Indicator – real-time phone scam detection and prevention, launched in October 2023. Built in collaboration with Quantium Telstra, Scam Indicator is helping to prevent phone scams targeted at joint CBA/Telstra customers;
- Intelligence sharing pilot – near real-time SMS scams intelligence sharing with Vodafone, allowing the telco to identify and disrupt scammers, while the bank may implement proactive blocks on suspected fraudulent payments; and
- Call Stop – sharing phone numbers, identified as being used to facilitate scam calls and SMS, with Optus for blocking or call redirection. This intelligence sharing is occurring via the Australian Financial Crime Exchange's (AFCX) Anti-Scam Intelligence Loop.

We welcome the opportunity to continue working alongside the Government, telecommunications sector, law enforcement, and other industries to combat scammers and implement solutions that better protect consumers.

This submission outlines CBA's responses to the consultation questions raised in the Consultation Paper and we would welcome the opportunity to discuss these further.

[1] National Anti-Scam Centre (NASC) Scam statistics (2023), available at: <https://www.scamwatch.gov.au/research-and-resources/scam-statistics?scamid=31&date=2023> (accessed 15 March 2024).
[2] July 2023 – December 2023.

2. Consultation questions

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

Scammers imitating companies' alphanumeric sender IDs (alpha tags), to insert fake messages into an existing SMS chain of a genuine business, have targeted CBA and our customers, along with many other businesses across the economy.

This method used by scammers deceives consumers and gives them the impression that they are dealing with a genuine business, putting consumers at risk of engaging with the message and ultimately the scammer.

These phishing/smishing scams are widely seen, with recent examples involving Linkt and AusPost, as well as financial institutions, amongst others. Further, it has been reported that more than 47 per cent of Australians have reported exposure to fake or deceptive text messages.[3]

The Registry will be an important tool for telecommunications providers to prevent spoofing of alpha tags via their networks.

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

CBA supports the introduction of a mandatory Registry for alpha tags and is participating in the pilot announced in December 2023. CBA also welcomes the Registry being underpinned by enforceable rules applied to telecommunications providers, as proposed in the Consultation Paper. To help address the misuse of alpha tags, telecommunications providers and mass SMS service providers should be required to remove this method for a scammer to initiate contact and deceive consumers.

A mandatory approach to protect alpha tags is critical, as whenever there are gaps in a solution to combat scammers, it provides them with the opportunity to adapt their methodologies to target these weaknesses. In this case, a voluntary approach will likely see scammers target the alpha tags of brands and entities not participating in the Registry, placing the customers of those brands and entities at a higher risk of being scammed.

It is also important to create a consistent approach for consumers, to help them identify attempts to scam them and to be confident when interacting with digital channels and communications. The Registry will help to create more trust and engagement with messages sent with alpha tags, noting however that small businesses are more reliant on SMS and may not use alpha tags.

The Registry will help telecommunications providers prevent the misuse of their services and reduce the ability for scammers to contact and deceive consumers. The Registry therefore will play an important role in the Government's whole of ecosystem approach to combatting scammers and providing greater protections for consumers.

2.3 What, if any, transition arrangements are required?

We encourage the broadening and mandating of the Registry as soon as possible and preferably by the end of 2024. We note that the Consultation Paper outlines that legislation will be required to implement a mandatory approach. However, we urge the Department to ensure that this does not

[3] Australian Government, *SMS Sender ID Registry set to protect more Australians from scammers,* (December 2023), available at: <https://minister.infrastructure.gov.au/rowland/media-release/sms-sender-id-registry-set-protect-more-australians-scammers>

delay the implementation of the Registry and suggest that the Registry be implemented on a voluntary basis in the interim, with the notion that it will become mandatory once the legislation supporting it is enacted. This will help provide greater protection for consumers in the interim and enable learnings to be incorporated from the voluntary phase.

With a mandatory model, it will be important for an education and awareness campaign to be implemented to inform businesses about the Registry and the importance of registering their alpha tags. It is also important that there is a national campaign to notify and educate consumers about these new changes, and how to differentiate between genuine and fraudulent text messages.

3. Additional considerations

To further limit the communication channels available to scammers, we suggest the following items be considered when implementing the Registry:

- *Blocking of messages* – where messages have been identified outside of a registered whitelist for an alpha tag, we suggest the telecommunications provider be required to block the messages and notify the impersonated business that the message relates to. That is, the messages should not be allowed to proceed without the alpha tag registered by that business.
- *2 Way SMS and SMS short codes* – in the case of 2 Way SMS, banks typically use these to confirm with a customer that a transaction on their account was made by them (typically requiring a Y or N response from the customer). These message types cannot be sent with alpha tags and, as such, we suggest the numbers used to send 2 Way SMS and SMS short codes should also be registered with the Registry to block the spoofing of these numbers.
- *Non-use of alpha tags* – we note that an unintended consequence of the Registry, and its associated costs, may be that some businesses no longer use alpha. This may undermine efforts to build confidence in digital communication channels, as consumers will receive messages from unknown numbers, making it difficult for them to identify a genuine communication. To counter this, where a business does not use an alpha tag, we suggest telecommunications providers should not allow the phone numbers used by these businesses to spam consumers by implementing limits on SMS volumes. This will incentivise these businesses to use and register alpha tags and help promote a consistent approach to SMS, which will assist consumers to identify whether a message is from a genuine and trusted organisation.

We suggest there should also be clear escalation pathways for entities to raise and remediate genuine communications that may have been inadvertently blocked.

Information sharing

As outlined in CBA's response to Treasury's Consultation Paper on the introduction of mandatory sector-specific scam codes, CBA suggests all entities operating within the proposed Scams Code Framework should be required to share scam intelligence on all incidences of scams, in a timely manner, through a trusted platform like the AFCX and its Anti-Scams Intelligence Loop. This would provide entities with a richer source of data to assist more timely investigations into confirmed scam activity and take the appropriate actions, such as blocking phone numbers from making further calls, blocking social media accounts, as well as initiating the trace and recovery of funds.

In relation to SMS, we suggest this central information-sharing platform can be leveraged by telecommunication providers to notify impersonated businesses of messages that have been blocked. The telecommunications provider should send the business a copy of the blocked message, so the business can enable others within the ecosystem to investigate additional intelligence and take appropriate action in response such as malicious website takedowns.