OPTUS

Submission in response to DITRDCA Consultation Paper

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

Public Version

March 2024

INTRODUCTION

1. Optus welcomes the opportunity to provide feedback to the Department of Infrastructure, Transport, Regional Development, Communications and the Arts' (the Department's) consultation paper, 'Fighting SMS scams -What type of SMS sender ID Registry should be introduced in Australia?' (the consultation paper).

2. The telecommunications industry has led the way in tackling scams, with the successful introduction of a mandatory telecommunications industry code, together with innovative technical features, over and above those required in the industry code, to disrupt scam activity.

3. These measures have focussed on two main aspects – blocking potential scam calls or SMS and making it easier for consumers to identify potential scam communication. This has already successfully disrupted scam activity, helped to protect key Australian brands, and reduced consumer losses to scams.

4. However, this has only been of benefit where businesses have actively engaged with the telecommunications industry. Not all businesses have adopted the same level of commitment to protecting their brands against impersonation scams. As a result of this, Optus has experienced some challenges in reducing scam communications impersonating some well-known brands.

5. Optus agrees that a mandatory SMS sender ID registry is necessary to have further success in reducing scam activity. Such registries have been successfully implemented overseas and can be commercially sustainable. It is important that such a registry be Government run, and the focus should be on keeping costs low.

6. A registry could be implemented in a phased approach which would enable monitoring and necessary adjustments to ensure effectiveness. Scammers will continue to evolve their activity and solutions in place, including the registry, should be flexible enough to respond.

7. Optus considers it is time for such a scheme to move beyond initial trials and expand into broad and scalable protections. Where brand-owners are not taking adequate steps to protect their brands from impersonation, Optus believes a mandated registration scheme is warranted to protect businesses and consumers.

8. Ultimately, Optus considers such a scheme will benefit not only consumers by reducing the amount of potential scam communication and making it easier for consumers to identify potential scam communication, but, will also benefit businesses, who can protect their brand and reputation and increase consumer trust in and engagement with their communication.

9. The Department's consultation paper seeks feedback on three main issues to inform their consideration of an SMS Sender ID registry, including:

    (a) whether organisations have been targeted by scam impersonation schemes using false alphanumeric sender IDs (alpha tags);

    (b) whether a registry should be mandatory; and

    (c) what, if any, transitional arrangements are required.

10. While there is no one solution to address the issue of scams, Optus believes a mandatory SMS sender ID registry would assist in addressing scam activity by reducing the amount of potential scam communication and improving the ability of consumers to identify scam communication.

11. Experience to date suggests that protecting alpha tags helps disrupt scam activity. Previously, scammers have attempted to deceive people by using alpha tags to impersonate well-known companies and government organisations. Recipients of these scam messages may not realise the message is not from the legitimate organisation and click on a link contained in the message or contact the scammer as per the message.

12. Optus has seen positive results in reducing scam messages by protecting its own brands' alpha tags, such as 'Optus' or 'Amaysim', and by implementing the Trusted Sources pilot program.

13. In relation to its own brands, Optus has previously detected significant volumes of likely scam messages using the word 'Optus' or 'amaysim' in the message alpha tag. Protections for Optus' own brands focus on controlling the source of all legitimate Optus messages and then blocking all SMS from external sources that contain the word 'Optus' in an alpha tag.

14. These different types of protections have been successful in reducing the amount of messages attempting to impersonate Optus/Amaysim messages and have assisted in disrupting scam activity.

15. Optus has extended these protections to Australian brands; both commercial and government.

16. **[CIC Begins]**

17.

18.

19.

20.

21. **[CIC Ends]**

22. Optus' experience shows there are clear benefits from implementing such protections for alpha tags and origination sources. However, to make the protections effective, a Sender ID registry would need to be mandatory.

REGISTRY MUST BE MANDATORY TO BE EFFECTIVE

23. In Optus' view a voluntary scheme would negate many of the benefits that could flow from a central database. Many prominent brands have shown an unwillingness to protect their brands against Scam SMS through the use of existing voluntary schemes.

24. Successfully protecting alpha tags currently depends on the origination of SMS traffic and its subsequent message path. Where these high-profile brands use many uncontrolled messaging paths, scam messages that impersonate legitimate SMS traffic blend in with legitimate messages and are difficult for CSPs to detect and block.

25. There have been challenges in trying to reduce scam messages for some well-known brands because of the message paths they adopt for their traffic. High-profile brands have been reluctant to protect their SMS Sender IDs, which have made them vulnerable to impersonation by scammers. It is clear that many brands appear unaware of their messaging providers and paths that their SMS transit to arrive on their customers' devices.

26. **[CIC Begins]**

   [CIC Ends]

27. Other brands have worked to standardise their messaging systems and routes, which has made it possible to Optus to provide protections under the 'Trusted Sources' pilot scheme. For example, there has also been an additional major bank that has demonstrated an immense interest in Optus' SMS Sender ID protections. There have been delays due to this particular bank needing to understand the systems and routes they have in place for their messaging; although, protections have been implemented in a phased approach.

28. Optus has made protections available, but there are still many prominent brands that have not taken up the offer of protection. A voluntary approach, such as what was demonstrated during the Trusted Sources pilot has shown that many brands still exhibit an unwillingness to protect their brand against scam messages. Where brand-owners are not taking adequate steps to protect their brands from misuse, Optus considers a mandated registration scheme is warranted to protect consumers.

A REGISTRY CAN BE SUCCESSFULLY IMPLEMENTED

29. It has already been demonstrated that the Trusted Sources pilot scheme has had an impact in reducing the amount lost by Australian consumers by reducing the amount of scam messages that reach consumers and making it easier for consumers to identify scam SMS.

30. Optus supports a mandatory, centralised registry with a rules-based approach. Centralised registries have been successfully implemented overseas, for example, in Singapore and the UK. Further the Singaporean model demonstrates that a registry can be implemented in a way that is commercially sustainable.

A registry should be centralised, government operated and rules-based

31. Optus has reviewed the models that are in use in the United Kingdom and Singapore and has the view that the Singaporean model is more robust, offering a greater level of protection against scam SMS.

32. The Singaporean model was established in March 2022, with a phased implementation. It is a mandatory scheme and once fully implemented will result in messages being blocked where the alpha tag and organisation are not registered. This is a whitelist approach to a registry scheme.

33. Optus considers the key aspects of an Australian registry should include:

    (a)   A centralised registry run by an Australian entity (preferably the Australian Government). A centralised SMS Sender ID Registry scaled across more businesses and organisations would reduce the amount of Scam SMS that arrives on customer devices. A Government-run registry (similar to ABN/ACN Registers) would add legitimacy to the scheme and help ensure participation. Commercially led solutions risk creating perceptions that it is run to benefit the owner of the registry rather than to protect Australian consumers and businesses.

    (b)   An iterative approach with phased implementation. The model should aim to deliver a capable system as soon as possible, building on the existing Trusted Sources pilot scheme, with the greatest number of C/CSPs encouraged to participate in the scheme. Further protections can be built into the system following the implementation phases, similar to the Singaporean approach.

    (c)   Rules against using an alpha tag not in the Registry.

    (d)   Only C/CSPs registered on the Registry would be permitted to send messages with alpha tags to Australian Mobile Service Numbers (MSNs).

    (e)   Alpha tags would be permitted to be registered by companies that have a legitimate purpose (valid use cases), as required now under the telecommunications industry's C661:2022 *Reducing Scam Calls and Scam SMS Code* (Reducing Scams Code);

    (f)   API access for near-real-time information contained within the registry is preferred;

    (g)   The ability for a company/organisation to delegate permission to a third party to send messages on their behalf, utilising a registered SMS Sender ID. This should be revokable at any time.

34. The registry does not need to allow trusted brands to register phone numbers as regulations already exist that would enable the ACMA to take action against C/CSPs that originate an SMS using a number for which the A-Party does not have Rights of Use.

35. The registry should also contain important information, such as, the company/organisation registrant of the SMS Sender ID, valid use cases for the relevant alpha tag (such as those use cases as per the Reducing Scams Code – Supplementary Information Industry Guideline) and relevant contact details.

36. Optus considers the above would be a robust approach to implementing a registry model in Australia that will be most effective in reducing scam messages to Australian consumers.

A registry can be commercially sustainable

37. Optus considers that a registry does not need to be high cost to run, nor for businesses to register their SMS Sender IDs. The registry could be operated on a cost recovery basis by a Government agency, with costs being recovered from companies registering SMS Sender IDs. This is consistent with cost recovery objectives where the beneficiaries of regulatory action incur the cost.

38. The Singaporean model has demonstrated a sustainable commercial model, with the beneficiaries of Sender ID protections (i.e. brand owners) paying a fee for the registration of

each alpha tag. MNOs have invested heavily in building the capabilities in blocking scam SMS and protecting alpha tags that are part of the Trusted Sources pilot and also in implementing requirements under the Reducing Scam Calls and Scam SMS Industry Code (Reducing Scam Calls Code).

39. Further cost burdens on MNOs would limit the useability of any registry. To date, the cost to protect Australians from scam traffic has largely fallen on MNOs, with businesses having largely avoided cost impacts. MNOs will still have significant costs to implement the registry into their systems, and this work has material benefits to the brands that are protected and the customers of those brands. Brand owners would incur little to no costs to participate in this scheme.

40. Optus considers the initial establishment and operational funding of the mandatory registry should fall upon a Government body, though the ongoing funding would continue through the onboarding and annual registration fees of companies/organisations that register their SMS Sender IDs. This is reflective of the commercial model of the Singaporean registry.

41. The registry is just one part of the solution ecosystem to protect Australian business brands. To ensure a sustainable ecosystem, part of each onboarding and annual registration fee should be paid by the registry to the MNOs, to contribute towards ongoing operational costs of these systems.

Transition arrangements will be needed

42. Optus submits that transition arrangements or phased implementation will likely be required, similar to the approach that the Singaporean model has adopted.

43. The Singaporean SMS Sender ID Registry is in a transition period where any non-registered use of an SMS Sender ID will be replaced with *"Likely Scam"*; after which messages from all non-registered users will be blocked and not delivered to end-users. A similar approach could be considered for Australia. This approach would serve to encourage any senders who failed to register their Sender IDs in the initial availability period, while providing a phased approach to establishing a registry.

44. There should be an initial registration period that is only open to high-profile organisations which are at greater risk to impersonation. This should include:

    (a)   Telecommunication providers who have been involved in the Trusted Sources pilot;

    (b)   Banks and other financial institutions;

    (c)   Government agencies and entities.

45. Following the initial registration period, registration should be opened to other organisations, with encouraging those large organisations who provide essential services or have large Australian customer bases to register initially to protect their brand and their customers.

ADDITIONAL CONSIDERATIONS

46. There are additional considerations related to implementing a Sender ID registry that Optus notes the Department may wish to take into account. This includes:

    (a)   Requirements should apply to SMS aggregators;

    (b)   Short codes are not a substitute for alpha tags;

(c)   It would not be practical to block all SMS containing URLs; and

(d)   Consumer education and broader engagement from Australian business will continue to be needed.

47.   These are discussed further.

Requirements should apply to SMS aggregators

48.   Optus submits that compliance with a registry should also be required for SMS aggregators, which often accept wholesale SMS traffic from any international sources. SMS aggregators are commonly used by businesses in sending out SMS traffic and if SMS aggregators were not subject to the requirements of the registry then those organisations that use SMS aggregators and their customers could be more vulnerable to being targeted by scammers.

49.   If the aggregator cannot guarantee the international messaging traffic is compliant with the requirements of an Australian SMS Sender ID Registry, the aggregator should not be permitted to bring the SMS traffic into Australia. MNOs should be able to refuse interconnection to CSPs that are not members of the registry.

Short codes are not a substitute for alpha tags

50.   Optus notes the consultation paper considers a risk of a mandatory registry that entities who had not registered their alpha tags would either have to stop using their alphanumeric sender IDs (and use a mobile number of short code instead), or register and pay to keep using them (p. 10). This suggests that short codes could be used in lieu of alpha tags.

51.   However, Optus notes there are concerns with such a suggestion. There are restrictions that would prevent short codes from being used in this way.

52.   Public short codes (including 13/1300/1800 numbers) cannot be used as an SMS Sender ID under the *Telecommunications Numbering Plan 2015* and the Reducing Scam Calls Code. Specifically, under these regulations, 13/1300/1800 numbers cannot be used to make outgoing calls and alphanumeric sender IDs must not present as a number. There are also restrictions that would prevent the use of Telco Short Codes

53.   As such, short codes could not be used as a substitute for alpha tags.

Not proportionate to block all SMS containing URLs

54.   Optus considers that there are valid uses of URLs in SMS and it would be a disproportionate response to block SMS that includes a URL.

55.   The use of legitimate URLs in SMS is common across most businesses and government agencies. For example, URLs are used by businesses and government agencies in order to manage Spam Act requirements and to give customers the option to go to a website to opt out of receiving messages. Police forces include URLs in emergency notification messages. Postal companies send URLs to track packages. Health agencies include URLs to share valuable public health messages and consumers book medical and other appointments through URLs in SMS. Other typical business uses include links to invoices and receipts to links in marketing material.

56.   With so many legitimate uses of URLs in SMS, a blunt rule banning URLs in text bodies would have no net benefit. However, scammers have taken advantage of the legitimate reasons for URLs to be included in SMS when sending SMS impersonating such organisations to get consumers to click on fraudulent links.

57. While Optus has implemented a filtering capability that allows interrogation of the integrity of the URL with malicious links being blocked by such technology, a more robust approach would be a mandatory Sender ID Registry that restricts messages that are not from registered alpha tags.

58. The use of any non-registered Sender ID would be blocked, which would restrict the ability of scammers to impersonate known brands. This would make it clearer to individuals as to where the SMS originated; allowing them to make a better informed judgement as to whether a URL in a message presents as elevated risk.

Consumer education and business engagement will continue to be important

59. Optus considers that business engagement and consumer education about scam activities and identifying scam messages will continue to be important.

60. Consumers may still receive messages. Once a registry has been implemented, government should educate consumers about the scheme, what will be occurring, and what consumers should expect. In addition, where businesses take steps to protect their alpha tags they should educate their customers about the steps they take to minimise scams messages.

61. Scammers will always evolve and switch their methods. Telecommunications providers cannot be solely relied upon to combat scams. There is also a critical role to be played by other industries and for continued education of consumers to improve their ability to identify scam activity.