SMS Sender ID Registry – Fighting SMS Impersonation Scams

ACCC submission

19 March 2024

Introduction

The Australian Competition and Consumer Commission (**ACCC**) welcomes the opportunity to comment on the Consultation paper: *Fighting SMS Scams- What type of SMS sender ID registry should be introduced in Australia?* released by the Department of Infrastructure, Transport, Regional Development, Communications, and the Arts on 18 February 2024 (**Consultation Paper**).

The ACCC endorses the introduction of a mandatory Sender ID Registry (**Registry**) for alphanumeric Sender IDs in SMS messages.

The harm to consumers from SMS scams is clear. Reports to Scamwatch show SMS is the most common method used by scammers to approach potential victims. In 2023, Scamwatch received 109,616 SMS scam reports, which is an increase of over 37 per cent on the preceding year. Of these contacts, consumers reported losses of almost $27 million.

In a detailed analysis of Scamwatch reports in preparation for Scams Awareness Week 2023, the ACCC found that 72.5 per cent of scams from 1 January 2023 to 30 September 2023 involved an impersonation component. This demonstrates the risks of a Sender ID landscape where trusted business names are impersonated by scammers to contact potential victims.

The objective of any system needs to ensure that consumers can trust the messages they receive with a Sender ID and easily identify those that might be scams. Combined with education messages this will provide significant protections to Australians.

Recommendations

1. The ACCC supports the introduction of a mandatory SMS Sender ID Registry for alphanumeric sender IDs.
2. SMS messages that do not pass the checks required by the SMS Sender ID Registry model should be blocked.
3. A mandatory SMS Sender ID Registry must be backed by strong enforcement powers for the Australian Communications and Media Authority (**ACMA**).
4. Introduction of a mandatory model and related legislative changes should provide for a transitional period of at least 6 months for businesses to prepare.
5. Consumer education should raise awareness of the SMS Sender ID Registry

The ACCC and the National Anti-Scam Centre

The ACCC is an independent Commonwealth agency that promotes competition, fair trading, and product safety for the benefit of the Australian community. The ACCC's primary responsibilities are to enforce compliance with the *Competition and Consumer Act 2010* (CCA), regulate national infrastructure, and undertake market studies.

In 2023, the Government allocated $58 million over 3 years to establish the National Anti-Scam Centre within the ACCC to make Australia a harder target for scammers. The National Anti-Scam Centre commenced on 1 July 2023 with a focus on three key capabilities:

- **Collecting and sharing data and intelligence** across the scam ecosystem to enable the early identification of scam trends. This intelligence, shared with law enforcement, government departments and agencies, consumer groups, and the

private sector, will inform education and disruption efforts, focusing on early intervention to reduce or prevent losses to scams.

- **Coordinating scams prevention, disruption, and awareness activities** by drawing on expertise across government, law enforcement, industry, and consumer organisations to lead a nationally coordinated, timely, anti-scam strategy.
- **Helping consumers spot and avoid scams** by working with the National Anti-Scam Centre partners across the scams ecosystem to support consistent messaging and provide better education resources to help consumers protect themselves and others.

Consumer harm from scams where SMS was the primary contact method

Financial loss

Scams are a significant threat to Australian consumers and businesses, with financial losses to scams totalling at least $3.1 billion in 2022, a 76 per cent increase on losses recorded in 2021.[1] In 2022, 65 per cent of Australians were exposed to a scam attempt.[2]

In 2023, total reported losses to Scamwatch were $476 million. These figures reflect Scamwatch data only. We know that actual losses will likely be even higher given the many consumers who do not lodge a report for various reasons, including feelings of shame, unawareness of reporting options or processes, or belief the agency reported to would not be able to assist. The ACCC's Targeting Scams Report, which we expect to be released in April, will include combined 2023 losses reported to Scamwatch, ReportCyber, the Australian Financial Crimes Exchange, IDCARE, and Australian Securities and Investments Commission (ASIC). In 2022, combined losses reported to these entities were over $3.1 billion as noted above.

SMS is the most common method used by scammers

Based on reports to Scamwatch, SMS is the most common method used by scammers to approach potential victims. In 2023, there were 109,616 reports received where SMS was the contact method, an increase of over 37 per cent on the preceding year. Of these contacts, consumers reported losses of almost $27 million.

SMS scams are a profitable business model for scammers and initiatives to prevent scammers using SMS to impersonate legitimate business are limited. Based on Scamwatch reports from 2023, scams where SMS was the primary contact method were heavily focused on 'phishing' – that is, obtaining user credentials. Of the 109,616 reports where the primary contact method was SMS, 50 per cent were classed as phishing scams. While the average reported loss to SMS phishing scams was $97 for all reports including those without a financial loss, this figure does not represent the true extent of this type of scam. User credentials are of very high value to scammers in a scheme called 'credential stuffing', where the credentials of one compromised instance are used across multiple sites leading to data breaches of multiple organisations and potentially further financial losses.

[1] Targeting scams: Report of the ACCC on scams activity 2021 and Targeting scams: Report of the ACCC on scams activity 2022

[2] Australian Bureau of Statistics (2021-22), Personal Fraud, ABS Website, accessed 3 March 2024.

Scamwatch reports are therefore likely to significantly underestimate the harm from SMS scams, as a phishing SMS is often just the first stage in a long-running and multi-pronged scam.

Emotional and social harm

Reports to Scamwatch highlight the significant emotional and social harm caused by scams. Many Australians report losing their entire lifesavings; their superannuation; their home and their families. The ACCC has been made aware of Australians who have died by suicide as a direct result of a scam.

A mandatory SMS Sender ID Registry

With such significant harm from SMS scams, the ACCC considers a mandatory Registry is the best way to mitigate this harm and provide comprehensive protection for consumers. Importantly, only under a mandatory Registry can consumers trust that an SMS sender is who they say they are across all messages they receive. This is essential to an effective model.

This is also consistent with international approaches. For example, Singapore's Sender ID Registry was made mandatory from 31 January 2023 after the introduction of a voluntary regime in March 2022. We understand 120 organisations registered during the voluntary phase, while over 4000 organisations registered in the mandatory phase. As of December 2023, 97 per cent of A2P (application to person) SMSs sent in Singapore are with registered Sender IDs. We understand early results are extremely encouraging.

A mandatory Registry will lower costs to each entity as the cost recovery of the Registry would be spread across more participants. This avoids the deterrent effect of a voluntary registration model that is likely to have higher costs to individual participants and may not be feasible for a smaller number of entities.

A mandatory Registry also makes it easier for businesses to comply and operate on an even playing field. In contrast, a voluntary model would continue to allow scammers to prey on weaknesses in the system to continue to impersonate businesses.

Importantly, a voluntary Register does not adequately address or protect the needs of:

- Consumers – who would not know which brands and entities are protected and which entities are not, leaving them vulnerable to scams and/or distrustful of all SMS's. This would make attempts to tackle SMS scams less effective.
- Businesses who voluntarily register – registration would have less value because consumers will not have full trust in the Register. Non-registered businesses may also free-ride on any trust and legitimacy created by the investment of registered businesses.

The ACCC considers a mandatory Registry represents a targeted measure that is likely to make it harder for scammers to prey on consumers via the use of SMS, while enabling legitimate businesses to continue to utilise SMS as a method to communicate with their customers. As noted by the ACCC in the draft report for the current inquiry on whether to declare the mobile terminating access service, effective targeted measures, to detect and combat scams, are likely to better promote efficient use of telecommunications infrastructure than the blunt tool of raising commercial prices for A2P (application to person) SMS termination.[3]

[3] 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, p. 74.

In addition to its mandatory nature, key elements of an effective Registry include:

- Clear enforceable obligations
- A verification process for the Registry that is robust and rigorous. For example, this could reduce issues associated with potential variations that are used to try and imitate legitimate brands (for example, ComBank vs Commbank).
- Adequate enforcement powers and resources
- SMS blocking (discussed further below).

Blocking SMS messages

The ACCC supports blocking SMS messages that do not pass the checks required by the Registry model rather than marking them 'fraudulent'.

Drawing on international experience, in Singapore only registered Sender IDs are allowed, while the use of all other non-registered Sender IDs are blocked, which means non-registered Sender IDs are converted to and marked 'likely-SCAM'.

The rational behind converting non-registered Sender IDs to 'likely-SCAM' rather than blocking the SMS message is to minimise disruption to two groups of users Singapore has identified: (1) locals travelling overseas who may receive SMS from businesses overseas; (2) Foreigners working in Singapore who still receive SMSs from their country of origin, for example SMSs from banks or the government.

Converting non-registered Sender IDs as 'likely-SCAM' has value, however scammers have a high level of ingenuity and Scamwatch receives many reports from consumers who are manipulated into reading one-time passwords over the phone to scammers, even when the password message includes a prominent warning. There are similar risks that scammers will use social engineering to manipulate consumers, even where SMSs are marked 'likely-SCAM'. For example, consumers are regularly told to 'check their junk or spam mail folders' for legitimate emails, in the same way scammers could suggest to consumers that legitimate SMSs are being marked 'likely-SCAM' and consumers should disregard the warning.

Many consumers will also read the message and make their own determination about whether a message is a scam or not. Techniques used by scammers, including fear and urgency, may mean the warning is ignored.

The ACCC considers blocking SMS messages will be more effective than marking them with a warning message. In the UK, their SMS Protection Registry is an industry led initiative comprising of more than 30 banks and government agencies participating with over 520 registered Sender IDs. This initiative has been responsible for blocking over 2400 unauthorised variants of registered organisations' names. Where messages are not using a Sender ID that is authorised by a merchant or brand the message is blocked as fraudulent, ensuring SMS remains a trusted communication channel for brands and consumers alike.[4]

However, if it is not possible to block messages, the messages should be marked 'likely-SCAM'.

[4] Mobile Ecosystem Forum, https://mobileecosystemforum.com/sms-senderid-protection-registry/, accessed 19 March 2024.

Mandatory Registry should be backed by strong enforcement powers

Effective enforcement, backed by substantial penalties for non-compliance, must form part of a mandatory Registry to ensure compliance is a priority for all telecommunications providers.

The ACCC understands that application-to-person SMS service providers and SMS aggregators that originate SMS may not have the same incentives as the mobile network operators to filter out scam SMS. For example, their volume-based business models mean they likely have strong incentives to send as many messages as possible, and the intended recipients of the SMS are not directly their customers.

As such, the ACCC considers the legislative framework establishing a mandatory Registry should provide strong enforcement powers for the ACMA, requiring telcos to use the Registry to ensure that the SMS sender has a legitimate case for using a particular Sender ID. The ACMA has already issued a number of directions to some application-to-person SMS service providers for breaching anti-scam rules under the Reducing Scam Calls and Scams SMS Industry Code.[5]

Transition process

The ACCC considers introduction of a mandatory model and related legislative changes should provide for a transitional period of at least 6 months for businesses to prepare, register, or make any necessary changes to their businesses in order to participate. This transitional period is intended to avoid the unintended effect of legitimate SMSs being blocked for entities that may not have been able to register.

As some organisations may need more time to prepare and register there may be benefit in a phased approach to compliance. Higher risk sectors, such as banks, may be prioritised for mandatory registration sooner than other sectors.

Mandatory Registry should be supported by consumer education

An education program aimed at consumers is essential to the success of a Registry. Many consumers are already wary or sceptical of SMS purporting to be from legitimate business due to the prevalence of SMS scams over recent years. Educating consumers that they can trust SMS messages are true to label, once the Registry is established, will ensure the Registry meets its intended objective.

[5] ACMA, *Telcos breached for allowing SMS scams*, May 2023, Entities: Sinch Australia Pty Ltd, Infobip Information Technology Pty Ltd and Phone Card Selector Pty Ltd; ACMA, *Burst SMS breached for allowing scams*, August 2023, Entity: Known Pty Ltd (trading as Burst SMS); ACMA, *Five telcos breached for allowing SMS scams*, February 2024, Entities: Message4U Pty Ltd (trading under the brand name Sinch MessageMedia), SMS Broadcast Pty Ltd, DirectSMS Pty Ltd, Esendex Australia Pty Ltd and MessageBird Pty Ltd.