Australian Government
Department of Infrastructure, Transport,
Regional Development, Communications and the Arts

# Fighting SMS impersonation scams: the SMS Sender ID Register model for Australia

## Impact Analysis

**November 2024**

Director – Publishing and Communications
Communication Branch
Department of Infrastructure, Transport, Regional Development, Communications and the Arts
GPO Box 594
Canberra ACT 2601
Australia

Email: publishing@communications.gov.au

Website: www.infrastructure.gov.au

# Table of Contents


**Executive summary** 6

Introduction 6

Post-consultation analysis 7

Recommended option 7

The Impact Analysis process 7

**1. What is the problem, and what data is available?** 8

Impact of scams across consumer groups 8

SMS scams 10

Scale of SMS scams 10

Appeal of SMS for scammers 11

The rise of AI 11

SMS impersonation scams 12

Impact on Australian consumers from SMS impersonation scams 13

Damage to Australian businesses from SMS impersonation scams 14

Harm to the digital economy from SMS impersonation scams 16

**2. What are the objectives, why is government intervention needed to achieve them, and how will success be measured?** 18

What are the objectives? 18

Why is government intervention needed? 18

Action taken to date 19

Blocking of scam SMSs 19

Compliance action undertaken 20

SMS Sender ID Register pilot 20

Limitations of existing measures 21

Operation of the Register pilot 21

Need to establish an enforceable, industry-wide model 21

Overseas regulators recognise the need for intervention 21

Not a 'silver bullet' solution 23

**3. Policy options considered** 24

Option 1: Status quo (no change) 24

Option 2: Voluntary registration of SMS sender IDs 25

Advantages and disadvantages of voluntary registration 25

Option 3: Mandatory registration of SMS sender IDs 26

Advantages and disadvantages of mandatory registration 26

**4. What is the likely net benefit of each option?** 27

Data collection 27

Primary data collection 27

Secondary data collection 28

Methodology 28

Cost inputs 29
Benefit inputs 29
Timeframe 29
Option 1: Status quo (no change) 29
Costs 29
Option 2: Voluntary registration of SMS sender IDs 30
Costs 30
Benefits 34
Total benefits – voluntary registration 38
Total net benefit: voluntary registration 39
Option 3: Mandatory registration of SMS sender IDs 40
Costs 40
Benefits 42
Total benefits: mandatory registration 44
**5. Who did you consult and how did you incorporate their feedback? 46**
Targeted consultation: February 2023 46
Summary: outcomes of consultation 47
Public consultation: February-March 2024 47
Businesses/organisations 47
Individuals 48
Who contributed their views to the consultation? 48
Summary of key feedback from the public consultation 48
Key themes emanating from consultation 49
Consultations conducted as part of cost-benefit analysis: July-August 2024 51
Targeted consultation 51
Business and consumer surveys and focus groups 51
Further opportunities for consultation 52
Conclusions 52
**6. What is the best option from those you have considered and how will it be implemented? 53**
What is the best option? The Decision Rule 53
Option 1 – Maintain the status quo (no change) 53
Option 2 – voluntary registration of sender IDs 53
Option 3 – mandatory registration of sender IDs 53
Preferred option 54
Implementation 57
Measures to support implementation 57
**7. How will you evaluate your chosen option against the success metrics? 59**
Measurement of success 59
Measurable indicators 59
SMS blocking vs a decrease in the initiation of SMS sender ID impersonation scams 59
Other indicators 60

Monitoring and evaluation 60
Collection of new datasets by the NASC 60
Ongoing evolution of the success metrics 61
**Abbreviations and Glossary 62**
**Appendix A – Cost-Benefit Analysis 63**

# List of Figures and Tables

Figure 1: Combined Scams Losses—2020-2023 8
Figure 2: Scam Reports and Losses by Age Group 9
Table 1: Contact mode for scams – Reports and losses 11
Figure 3: The scam SMS message below appears in the same threads as legitimate SMS messages 13
Table 2: Differences in financial losses to SMS scams between groups. 14
Figure 4: Staff time (organisations/entities) resolving complaints from SMS impersonation 15
Figure 5: Customer disengagement due to SMS scams 15
Figure 6: Trust index – Communications channels in Australia and New Zealand 17
Figure 7: Total Scam Calls and Scam SMS Reported Blocked 20
Figure 8: SMS scam impersonating St George Bank in the body of the SMS message 23
Figure 9: Model structure to define categories of costs and benefits inputs for the CBA 28
Table 3: Total monetised harm associated with sender ID impersonation scams. 30
Table 4: Australian Government 2023-24 Budget allocation for SMS Sender ID Register. 31
Table 5: Indicative telecommunication industry participants costs. 32
Table 6: Sender ID user costs of registration. 33
Table 7: Sender ID user costs: voluntary registration. 33
Table 8: 2023 Financial losses from sender ID impersonation scams. 35
Table 9: Time spent resolving sender ID scams. 35
Figure 10: Responses to the Question: How much time did you spend trying to resolve issues caused by the scam SMS? 36
Table 10: Nuisance cost of alphanumeric sender ID scams. 37
Table 11: Time spend resolving customer complaints. 38
Table 12: Average annual regulatory costs (from businesses as usual), undiscounted over 10 years. 38
Table 13: Total benefits for voluntary registration, NPV over 10 years at a 7% discount rate. 39
Table 14: Net Present Value (NPV) over 10 years ($ million) for voluntary registration. 40
Table 15: Sender ID user costs: Mandatory registration. 42
Table 16: Average annual regulatory costs (from businesses as usual), undiscounted over 10 years. 42
Figure 11: Share of consumers reporting changing behaviour in response to SMS scams 43
Table 17: Total benefits, NPV over 10 years at a 7% discount rate - Mandatory registration. 44
Table 18: CBA calculation for mandatory registration, NPV over 10 years at a 7% discount rate. 45
Figure 12: Willingness of businesses/organisations to pay to register SMS with alphanumeric sender IDs 49
Table 19: Key themes from 2024 consultation by the Department. 50
Table 20: Organisation survey respondents (that use sender IDs), response to question: In your view, should registration by sender ID users be mandatory or voluntary? 51

Table 21: Primary results of the CBA, comparing voluntary and mandatory registration, net present value (NPV) over 10 years ($ millions). 54
Table 22: Comparison: Mandatory registration and voluntary registration against register objectives. 56

# Executive summary

## Introduction

The Australian Government is committed to making Australia a hard target for scammers.

An SMS sender ID Register (**Register**) which protects alphanumeric sender IDs is part of the government's suite of initiatives to combat scams and to protect Australians from financial harm.[1]

The Australian Communications and Media Authority (**ACMA**) has been provided funding to establish and maintain the Register.[2]

The Register aims to protect consumers and brands by disrupting a specific type of SMS impersonation scam, where scammers send SMS with alphanumeric sender identifications (**IDs**) to imitate well-known brands such as banks, government agencies or retailers in order to deceive victims, to steal their money or personal information.

Once operational, the Register will accept applications from, and store the sender identifications of, legitimate entities and businesses.

The ACMA commenced a voluntary pilot for the Register on 15 December 2023 that consolidated and centralised existing provider-level initiatives to protect participating alphanumeric sender IDs from impersonation by scammers. During 2024, the ACMA has expanded the pilot and contacted further providers and brands to discuss participation. Lessons from the pilot will assist to inform the Register's implementation.

The Telecommunications Amendment (SMS Sender ID Register) Act 2024 received Royal Assent on 5 September 2024 and will commence on a day to be fixed by Proclamation, or no later than 6 March 2025. The ACMA must establish the register 'as soon as practicable' after the Act commences. The legislation provides:

- a legislative basis for the ACMA to establish and maintain the Register; and
- powers that will allow ACMA to make determinations in relation to applications to register sender IDs, accessing the Register, and the administration and operation of the Register.

Whether the Register's end state is voluntary or mandatory registration for SMS sender IDs does not feature in the legislation, and will be a question to be determined by the Government later in 2024. The estimated regulatory impacts for both voluntary registration and mandatory registration which form the basis of this Impact Analysis will be presented to the Government to inform that decision.

To estimate regulatory impacts, the Government engaged Deloitte Access Economics to conduct an analysis of the costs and benefits associated with both registration options. The analysis indicates that the benefits outweigh the costs for both mandatory registration and voluntary registration, with mandatory registration delivering a greater net benefit. The costs of both registration options are similar but under the mandatory option, consumers receive $192 million in benefits from avoided financial costs and avoided time spent resolving scams, while sender ID users receive $65 million in benefits.

---

1 Department of Infrastructure, Transport, Regional Development, Communication and the Arts (Aust), 'Albanese Government acts to disrupt illegal text message scams' (Web Page, 23 April 2023), <https://minister.infrastructure.gov.au/rowland/media-release/albanese-government-acts-disrupt-illegal-text-message-scams>.

2 Budget 2024 – 2025, 'Budget Measures, Budget Paper No.2' (14 May 2024) <https://budget.gov.au/content/bp2/download/bp2_2024-25.pdf>.

The implementation of a Register framework that increases protection to brands and consumers would have an immediate and positive effect for Australians in disrupting SMS impersonation scams. It would also have positive flow-on impacts for SMS as a mode of communication. The pervasiveness of SMS scams over the last few years has generated significant distrust of SMS messages. Restoring consumer trust in SMS communications sent by businesses and entities is expected to have wide-reaching effects for the economy.

However, the government is cognisant that such a framework must be carefully calibrated to avoid imposing unreasonable or unintended burdens on businesses and entities registering their sender IDs. An overly onerous framework could result in an unreasonable impost on certain sectors, and even discourage business and entities from utilising SMS as a communications tool.

# Post-consultation analysis

The development of the recommended option has taken into consideration:

- the views of stakeholders provided during three consultation processes conducted in 2023 and 2024; and
- a cost-benefit analysis (**CBA**) conducted by Deloitte Access Economics (**DAE**) to estimate the costs and benefits of both voluntary and mandatory registration of SMS sender IDs.

# Recommended option

The recommended model sought is one which supports the achievement of the policy objectives while addressing stakeholder needs.

Option 3, the mandatory registration model, presents the greatest net benefit and most effectively delivers on the regulatory objectives associated with preventing SMS Sender ID impersonation scams. This option effectively addresses the Government's commitment to safeguard consumers and entities against SMS sender ID impersonation scams by protecting the legitimacy of SMS sender IDs.

Option 3, the mandatory registration model, is presented in this analysis alongside Option 2, the voluntary registration model and Option 1, the status quo.

# The Impact Analysis process

This IA has been prepared in accordance with the Australian Government IA requirements. In the subsequent chapters, the seven assessment questions set out in the Australian Government Guide to Policy Impact Analysis (2023) have been addressed.

Methods to determine the likely regulatory burden and costs and benefits were considered in the preparation of this IA. Information has been made available through consultation and through an additional cost-benefit analysis conducted by DAE.

The seven IA questions addressed are:

1. **What is the problem you are trying to solve and what data is available?**
2. **What are the objectives, why is government intervention needed to achieve them, and how will success be measured?**
3. **What policy options are you considering?**
4. **What is the likely net benefit of each option?**
5. **Who did you consult and how did you incorporate their feedback?**
6. **What is the best option from those you have considered and how will it be implemented?**
7. **How will you evaluate your chosen option against the success metrics?**

# 1. What is the problem, and what data is available?

Scams continue to devastate large numbers of Australians.

As a type of fraud, scammers find ways to exploit social and technological vulnerabilities in the ways Australians interact and do business in the digital economy. False offers of payments, employment opportunities, investments and fake notices may be targeted, and facilitate other types of crime, including identity theft and cybercrime. Bad actors impersonate trusted brands, service providers and websites, where the consumer may have previous or ongoing legitimate dealings.

The Government recognises the impact scams in general have had on Australian consumers and businesses and, as part of the 2023-24 Budget, provided $86.5 million over four years to deliver its commitment to combatting scams and online fraud, including:

- $58 million to establish the National Anti-Scam Centre in the Australian Competition and Consumer Commission (launched in July 2023)
- $17.6 million for the Australian Securities and Investments Commission to identify and take down investment scam and phishing websites, and
- $10.9 million over four years to launch and maintain a SMS Sender ID Register to help prevent scammers imitating key industry or government brand names in SMS message headers.

An additional $67.5 million was allocated to combating scams in the 2024-25 Budget, including $37.3 million to regulators to administer and enforce mandatory industry codes requiring banks, telcos, social media, digital messaging and search advertising services to have measures in place to prevent, detect, disrupt, respond and report scams.

There are tentative signs that action undertaken is working; recent reports to Scamwatch have indicated a decline in scam losses. Data released by the ACCC in April 2024 indicates that losses decreased by 13.1 per cent in 2023 compared to 2022. Mitigations by government have helped with loss reductions but with such a limited time span and data it remains too early for a definitive ongoing downward trend to be evident.

**Figure 1: Combined Scams Losses—2020-2023**


Source: Targeting Scams: *Report of the National Anti-Scam Centre on scams activity 2023*

However, while losses have decreased and progress is being made, Australians are still losing far too much. SMS scams in particular remain a highly utilised method by which scammers contact their victims. This is explored further in this chapter.

## Impact of scams across consumer groups

Scams affect all sectors of the Australian community. They lead to reduced consumer trust and confidence. For scam victims, these frauds are often devastating and life-changing.

Data published by Scamwatch for the initial six months of 2024 reveal that vulnerable community members are more susceptible to scams. Scammers often deliberately target vulnerable groups such as the elderly, migrants, and people with disability.[3]

Scams targeting specific groups or individuals are known as spear phishing.[4] Spear phishing focuses on specific targets, generally involves prior research and appears to come from a trusted source. For already vulnerable community members it is increasingly difficult to identify a scam.

Data published by the National Anti-Scam Centre[5] indicates that in 2023:

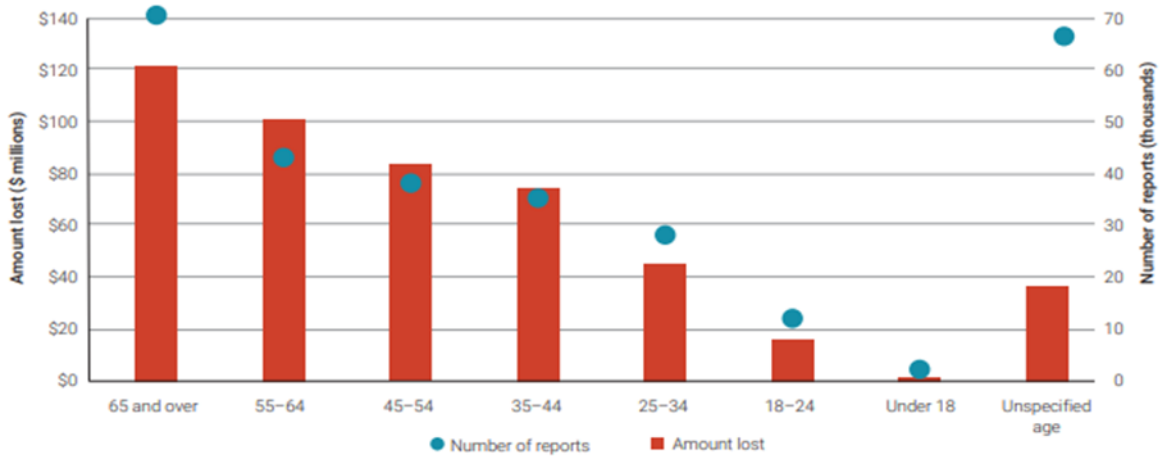
- older Australians (65+) experienced the highest financial losses from scams ($120.9 million)
- Indigenous Australians lost $3.7 million, and were over-represented in financial losses for identity theft and online shopping
- people with English as a second language lost $60.5 million, and were over-represented in financial losses for threat-based scams and unexpected money scams; and
- people with disability reported losses of $30.8 million, and were over-represented in health and medical scams and travel and prize scams.

Older Australians (65 years+) were most affected by these scams in terms of financial losses. Data from Scamwatch for the period 1 January to 30 June 2024, shows that individuals aged over 55 accounted for 48.7% of scam losses.[6]

Although there was a general decline in scam losses in 2023 compared to 2022, older Australians were the sole demographic that did not experience a decrease.

In 2023 individuals aged over 65 reported losses amounting to $121 million, the highest among all age groups.[7] This was an increase of 13 per cent from the previous year.

**Figure 2: Scam Reports and Losses by Age Group**




Source: *Targeting Scams Report 2023*

---

3 Australian Competition and Consumer Commission, National Anti Scam Centre, Scamwatch, *'Scams Awareness Week 2024 Key Statistics'* (August 2024) <https://www.scamwatch.gov.au/system/files/scams-awareness-week-2024-key-statistics_0.pdf>

4 *Glossary | Cyber.gov.au*

5 Australian Competition and Consumer Commission, *Targeting scams: Report of the ACCC on scams activity 2023* (April 2024) <https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf>

6 Australian Competition and Consumer Commission, National Anti Scam Centre, Scamwatch, *'Scams Awareness Week 2024 Key Statistics'* (August 2024) <https://www.scamwatch.gov.au/system/files/scams-awareness-week-2024-key-statistics_0.pdf>

7 Australian Competition and Consumer Commission, *Targeting scams: Report of the ACCC on scams activity 2023* (April 2024) <https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf>

There was also a 104% increase from 2020 to 2021 in reports to Scamwatch from people with a disability, and a 102% increase in financial losses. Media reports[8] have noted that people with disability are part of a growing target group for scammers. In 2023 Scamwatch received 22,080 reports (7.3% of total reports) from people with disability, with this group reporting financial losses of $30.8 million (6.5% of total losses). Despite reports increasing by 34.0%, losses decreased by 8.5%. Figures provided by the National Anti-Scam Centre for the first six months of 2024 as part of Scams Awareness Week show people with disability reported 11,367 scam reports and accounted for 5.9% of financial losses.

In 2022, First Nations Australians reported 3,889 scams, a number that increased to 6,192 in 2023. Despite the increase in reported incidents, the financial losses decreased to $3.8 million in 2023 from a higher figure the previous year. Between January and March 2024, First Nations people made up 1.6% of all scam reports and incurred losses amounting to $1 million, representing approximately 1.4% total losses for the period.[9] In the first half of 2024, the total number of scams reported by this group reached 2,318. Research suggests First Nations people may be hesitant to report any losses and NASC will be doing more work with Indigenous communities in this area. [10] Other reports also suggest there are additional barriers to reporting.

People from culturally and linguistically diverse communities (CALD) are another group experiencing over representation in scam victim numbers. In the period from July to December 2023, members of the CALD community reported losses totalling $24.94 million.[11] Throughout 2023 CALD members made 14,396 reports to Scamwatch, marking an increase of 26.1% from the previous reporting period. Reported losses amounted to $60.5 million which was an increase of 6.9%. Notably, members of the CALD communities experienced higher losses compared to the overall figures reported to Scamwatch. From January 1 to June 30, 2024, individuals with English as a second language submitted 6,588 scam reports, accounting for 17% of total financial losses reported in this timeframe.[12]

## SMS scams

SMS is still the most frequently reported contact method for scams, and almost $27 million was lost to SMS scams in 2023, as reported to Scamwatch[13]. The actual figure is likely to be significantly higher, as many scams go unreported.

## Scale of SMS scams

For the first 9 months of 2024, Scamwatch has documented a total of 68,734 SMS scams with financial losses amounting to $11,079,793. Only 1.6% of reporters suffered a financial loss, however 4.6% of reporters indicated they lost personal information to SMS scams. This difference highlights that impacts of SMS scams are not just financial, as victim personal information can be used for further scams or fraud[14].

---

8 Australian Competition and Consumer Commission, *Scam losses to culturally diverse communities, people with disability and Indigenous Australians almost doubled in 2021,* (Webpage, accessed 21 October, 2024) https://www.accc.gov.au/media-release/scam-losses-to-culturally-diverse-communities-people-with-disability-and-indigenous-australians-almost-doubled-in-2021

9 ABS data states that 3.8% of the Australian population are Aboriginal or Torres Strait Islander with 33% of these under 15 years of age.

10 Australian Competition and Consumer Commission, *Targeting scams: Report of the ACCC on scams activity 2023* (April 2024) <https://www.accc.gov.au/system/files/targeting-scams-report-activity-2023.pdf>

11 Ibid.

12 Australian Competition and Consumer Commission, National Anti Scam Centre, Scamwatch, *'Scams Awareness Week 2024 Key Statistics'* (August 2024) <https://www.scamwatch.gov.au/system/files/scams-awareness-week-2024-key-statistics_0.pdf>

13 Scamwatch, Scam statistics, (Webpage, accessed 24 August 2024) https://www.scamwatch.gov.au/research-and-resources/scam-statistics

14 Scamwatch, Scam statistics, (Webpage, accessed 22 October 2024) https://www.scamwatch.gov.au/research-and-resources/scam-statistics

Two thirds of Australians aged 15 years and over were exposed to a scam in 2021-22, and exposure to scams via SMS message doubled from 23% in 2020-21 to 47% in 2021-22.[15]

In 2023, SMS messaging was identified as the most frequently reported method of contact, with 109,621 reports made. This represents an increase of 37.3 per cent from 2022.[16]

**Table 1: Contact mode for scams – Reports and losses**

| Contact Mode | 2022 losses (m) | 2023 losses (m) | 2022 reports | 2023 reports |
|---|---|---|---|---|
| **Phone call** | $141.0 | $116.0 | 63,816 | 55,418 |
| **Social media** | $80.2 | $93.5 | 13,427 | 17,542 |
| **Email** | $77.3 | $80.0 | 52,159 | 85,941 |
| **Internet** | $73.5 | $69.7 | 13,692 | 17,568 |
| **Mobile apps** | $71.7 | $64.8 | 10,057 | 8,101 |
| **In person** | $30.6 | $21.5 | 2,186 | 3,614 |
| **Text Message** | $28.5 | $26.9 | 79,835 | **109,621** |

Source: *Scamwatch, 2023*

## Appeal of SMS for scammers

SMS is a universal technology supported by every mobile network and most devices.[17] ACMA research[18] shows that 91% of Australians reported using their mobile phone for SMS, second only to calls. SMS – and Multimedia Messaging Service (MMS) – can reach a recipient anywhere and at any time of the day where there is mobile coverage.

Furthermore, SMS is a popular channel for businesses to communicate with their customers; SMS messages are used for informing customers about ongoing promotions, closing periods, schedule changes and upcoming sales[19]. Australians have become accustomed to receiving SMS from businesses or organisations that they trust.[20] The popularity of SMS as a communication channel makes it an appealing tool for scammers to exploit. Accordingly, scams conducted via SMS continue to rise.

## The rise of AI

Knowing the difference between a scam SMS and a commercial marketing SMS is proving increasingly challenging as advances in artificial intelligence (AI) and chatbots allow scam SMSs to look legitimate – making

---

15 Australian Bureau of Statistics, *13.2 million Australians exposed to scams* (Media release, 22 February 2023) <https://www.abs.gov.au/media-centre/media-releases/132-million-australians-exposed-scams>

16 Australian Competition and Consumer Commission, Scam losses decline, but more work to do as Australians lose $2.7 billion (Media release 28 April 2024) <https://www.accc.gov.au/media-release/scam-losses-decline-but-more-work-to-do-as-australians-lose-27-billion>

17 Australian Communications and Media Authority, *Reducing the impact of SMS scams delivered via short message service (SMS) Regulation Impact Statement,* (Impact analysis, June 2022) https://oia.pmc.gov.au/sites/default/files/posts/2022/07/Publish%20Version%20-%20Reducing%20the%20impact%20of%20SMS%20scams%20FINAL%20Published.pdf

18 Ibid, p.5

19 Ibid, p.5

20 Australian Communications and Media Authority, *Reducing the impact of SMS scams*, *delivered via short message service (SMS) Regulation Impact Statement* (June 2022) <https://www.acma.gov.au/sites/default/files/2022-07/Reducing%20the%20impact%20of%20SMS%20scams.pdf>

these scams harder to spot.[21] Scammers are utilising generative AI to draft coherent messages, without spelling and grammatical errors, even using slang to try and dupe consumers.[22]

There has been an increase in AI-driven phishing attacks in Australia with research revealing that Australia is within the top 10 countries targeted by phishing scams.[23]

AI scams are now being used by criminals to enhance their success rate. They make scams more difficult to detect and increase how often consumers are being targeted.

> Put yourself in my shoes. You get an SMS from, say, Myer/David Jones, Harvey Norman, JB Hi-Fi, Bunnings, Officeworks, Tax Office, Centrelink, Education Provider, church, et al., that there has been a transaction, and you need to contact the company to authorise or deny. AI knows you too well and concocts a highly believable script for which even the best will fall [24] Ray Shaw

## SMS impersonation scams

Phishing scams involve scammers posing as a legitimate entity to trick consumers into giving out personal information. Personal information includes bank account numbers, passwords and credit card numbers.[25]

Smishing – phishing by SMS –is where criminals steal this information by sending a fraudulent SMS inviting consumers to click on links that take them to malicious websites where personal information is obtained or malware is unknowingly downloaded.[26]

A particularly problematic SMS phishing technique involves scammers impersonating well-known brands and government agencies by using the ***alphanumeric sender IDs*** of those entities.

**What is an alphanumeric sender ID?**

> All SMS received by consumers show a sender ID at the top of the SMS – a message header – that identifies who sent the message. Sender IDs can be alphanumeric (e.g. the name of a brands, such as 'NAB', 'CBA'), short-codes (e.g. 12345) or public numbers (e.g. 0401 xxx xxx).
>
> Alphanumeric sender IDs allow users to send SMS messages using a recognisable ID. Alphanumeric sender IDs are used by many well-known Australian brands and government agencies, so consumers can easily identify who the SMS is from.

*Note: An alphanumeric sender ID is not a phone number at the top of the SMS (in the message header); however, an alphanumeric sender ID may contain a number or symbol.*

---

[21] Generated text is fluent, well-written and unlike previous scam texts, does not contain typos, spelling and grammatical errors – often an obvious red flag in identifying fraudulent messages. It can easily be written in the style used by a trusted entity.

[22] Tom Stayner, Alex Anyfantis, *The days and times you're most likely to receive a scam in Australia,* SBS News, (Published, 29 June 2024) <https://www.sbs.com.au/news/article/the-days-and-times-youre-most-likely-to-receive-a-scam-text-in-australia/9idp6670t>

[23] Gordon Peters, *AI-driven phishing scams, attacks increase in Australia:researc*h, The Wire, (Published 28 May 2024) <https://itwire.com/business-it-news/security/ai-driven-phishing-scams,-attacks-increase-in-australia-research.html>

[24] Ray Shaw, (Webpage, 8 August 2024) AI scams - damned clever and hard to spot - Cybershack

[25] Australian Competition and Consumer Commission, *Phishing,* (Web Page, 2022) https://www.scamwatch.gov.au/stay-protected/attempts-to-gain-your-personal-information/phishing?date=2023

[26] Australian Communications and Media Authority, *Reducing the impact of SMS scams*, *delivered via short message service (SMS) Regulation Impact Statement* (June 2022) <https://www.acma.gov.au/sites/default/files/2022-07/Reducing%20the%20impact%20of%20SMS%20scams.pdf>

The ACMA has previously reported that people are far more likely to fall for a scam using a specific or trusted brand if they've already received a genuine communication from the business or organisation.[27] Psychologists refer to this feeling as 'illusory correlation', which happens when we see events as linked when they're not. Illusory correlation tends to confuse or relax our natural caution, making us more vulnerable to scams.[28]

Sender IDs are used to sort SMS within applications on smart phones, meaning a scam SMS may appear in otherwise legitimate SMS threads from businesses or government agencies. This makes it very difficult for consumers to identify a scam.

**Figure 3: The scam SMS message below appears in the same threads as legitimate SMS messages**


## Impact on Australian consumers from SMS impersonation scams

Financial losses to SMS sender ID scams compromise the financial independence and psychological wellbeing of victims. These scams are marked by their volume and frequency. Scammers are targeting consumers on a mass scale with increasingly plausible messages.

The impact of these scams on the Australian community is substantial. Consumer trauma as a result of fraud and identity crime has long-term effects. Despite concerted efforts by government, regulators and industry, these scams remain a significant threat to the financial and emotional wellbeing of Australians.

### Financial impacts

The cost-benefit analysis undertaken by Deloitte Access Economics indicated the financial impacts of SMS impersonation scams on consumers are significant (estimated at $26.6M for 2023) and that this is the largest individual harm. (DAE's CBA also calculated the consumer time and nuisance costs from dealing with these scams; this is discussed at pages 28 and 29.)

Consumer surveys undertaken by DAE as part of the CBA found that individuals who reported scams were losing an average of $246 per incident and that people with a disability face an increased risk of scams and higher losses per incident.

---

27 Ibid 6.
28 Ibid 6.

**Table 2: Differences in financial losses to SMS scams between groups.**

| Group | Average money lost | Proportion of cohort scammed |
|---|---|---|
| **Elderly (65+)** | $296 | 6% |
| **Has a disability** | $303 | 14% |
| **Overall (all responses)** | **$248** | **11%** |

Source: *Deloitte Access Economics 2024*

### Non-financial impacts

In addition to monetary losses, scams inflict emotional and psychological impacts upon victims, potentially creating long-term burden and costs. Those affected by these scams may face the resulting additional time, cost and psychological burden from the lack of clarity or responsibility for businesses to respond to reports of scams and provide support to victims.

**Case study: Bank impersonation scam – over $300,000 lost**

Niamh received an SMS from a scammer which used her bank's alphanumeric Sender ID and appeared in her regular chain of messages from the bank. It said she had been pre-approved for a $6,000 loan – this alarmed her as she had not applied for a loan. She called the number in the SMS believing she was speaking with her bank but it was a scammer. Niamh questioned whether the SMS was a scam. Lena, a scammer, said it wasn't a scam and that her account was compromised.

Lena said she would send an SMS to Niamh via her bank's SMS with a reference number to prove she was from the bank. Niamh received the SMS and was convinced that she was talking to her bank. Lena told her that a person was logged into Niamh's banking and that she needed to move quickly to transfer money to secure accounts.

Niamh moved $300,000 from her account but became uneasy. At this point, Lena told her it was a scam and said 'We are in Brisbane, come find me'. Niamh terminated the call and contacted the real bank fraud department.

Source: *ACCC, Targeting scams 2022*

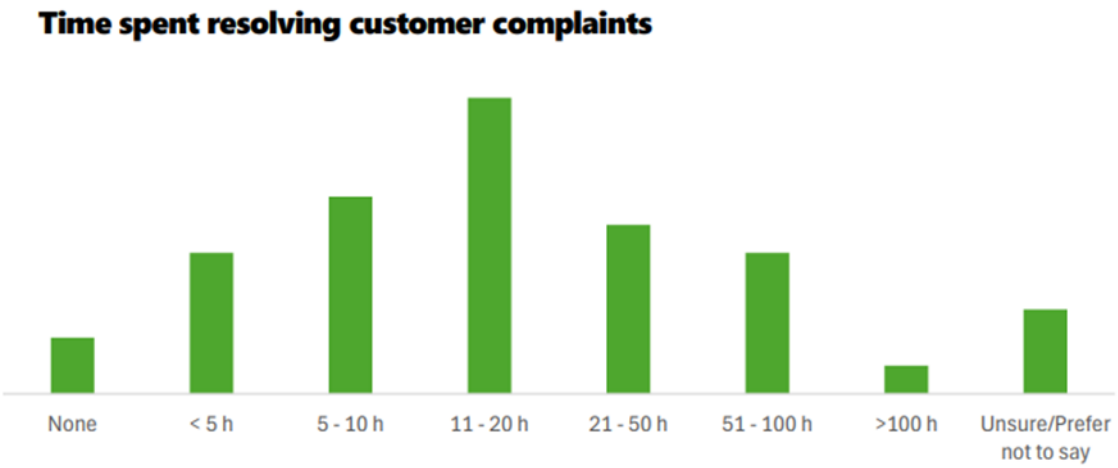
## Damage to Australian businesses from SMS impersonation scams

SMS impersonation scams are eroding the legitimacy of Australian businesses and brands.

In the last few years, these scams have affected the financial and reputational position of businesses and entities. Managing SMS impersonation scam-related risks means costs, and the diversion of staffing and resources into detecting, investigating and responding to these scams.

Insights provided by the CBA conducted by DAE indicate there is an estimated $19.8 million in wasted sender ID users' (businesses and organisations) time resolving issues and complaints from consumers experiencing SMS impersonation scams. This is based on findings from DAE business survey that indicate 31% of sender ID users spend an average 25 hours resolving customers issues related to SMS impersonation.

**Figure 4: Staff time (organisations/entities) resolving complaints from SMS impersonation**




Source: *Deloitte Access Economics 2024*

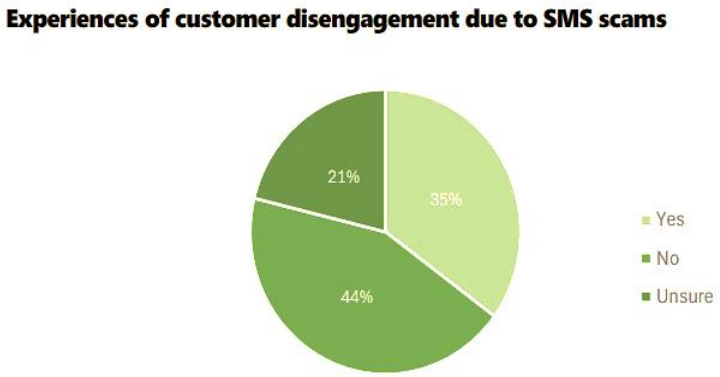
While the reputational impacts of these scams on businesses are difficult to quantify, SMS impersonation scams can severely damage the reputation of trusted brands.[29]

The Register's implementation is expected to significantly restore the level of trust in SMS communication to facilitate communication between trusted brands and their customers, ultimately saving both parties time and money.

Media reports[30] have commented that consumer experiences following scam contact often make the victim of the scam question SMSs from all organisations – legitimate or not.

Deloitte's survey findings of 2024 show businesses and entities that are impersonated by scammers may suffer loss of economic activity as consumers disregard legitimate dealings, or look to minimise risk by avoiding interacting with them. The same survey findings revealed that 35% of business who are current users of SMS sender IDs have experienced disengagement with customers due to scams.

**Figure 5: Customer disengagement due to SMS scams**




Source: *Deloitte Access Economics 2024*

---

[29] Brand Trust, *One Cyberattack is enough to lose consumer trust and custom,* (Webpage, 4 November, 2021) <https://mysecuritymarketplace.com/reports/brand-trust-one-cyberattack-is-enough-to-lose-consumer-trust-and-custom/>

[30] ABC News, *Drivers lose more than $660k to road toll scam as phishing attempts surge in Australia,* (Webpage News Report, 16 March, 2023) < https://www.abc.net.au/news/2023-03-16/toll-road-text-scam-targets-commuters-amid-phishing-surge/102087534>

## Harm to the digital economy from SMS impersonation scams

SMS is considered a 'communications heavyweight' – from an organisation's perspective, a direct, and cost-effective method to communicate compared to email, and social media posts.[31] For this reason, SMS has been a favoured method for communication by legitimate retailers and organisations.

Unfortunately, these benefits are also appealing to scammers. In addition, recipients of SMS scam messages cannot easily hover over a link in an SMS scam message (compared with a link sent via email)[32] to determine whether it is legitimate.

The harm generated by SMS impersonation scams and their increasing incidence present a significant risk to the operation of the digital economy. In short, impersonation scams conducted via SMS:

- undermine confidence in SMS as an effective communication channel
- may create a tendency for organisations and businesses to 'pause' SMS-based digital engagement[33]
- likely involve increased costs for industry issuing alerts to consumers to mitigate scam activity; and
- may lead to poor engagement and business outcomes, which has ramifications for the wider economy.

The importance of consumer trust and confidence in SMS as a communications channel cannot be underestimated. March 2024 research conducted by *Atomic.io' the State of Digital Trust* showed SMS as one of the least trusted channels for communication. This research surveyed over 1000 consumers in Australia and New Zealand [34]and sought views on preferred communication channels and their experience with scams and fraud.

The report includes a 'trust index' – which is calculated based on a range of behavioural and perceptual inputs, including general trust, confidence in preventing malicious activities, comfort with sharing sensitive information and frequency of checking message legitimacy.[35] Each channel's performance was measured across these metrics and then benchmarked against the average score across all channels to derive an overall index score.

---

[31] Whispir, *SMS Phishing scams bite but businesses can make things right,* (Webpage, 15 March 2022) <https://www.whispir.com/en-au/blog/sms-phishing-scams-bite-but-businesses-can-make-things-right/>

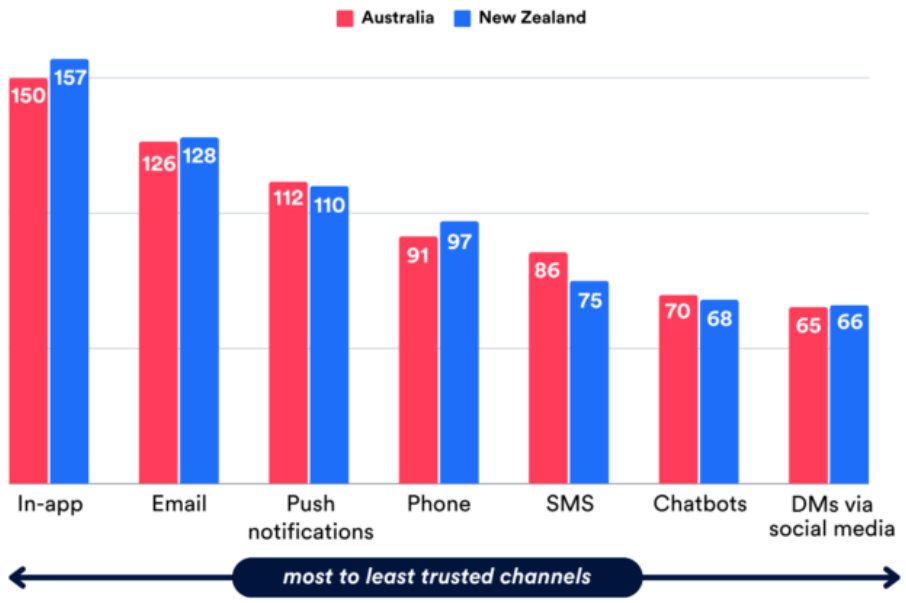
[32] Quantum Technologies *Dangerous Phishing Text Messages Are on the Rise. Learn What to Look Out For,* (Webpage, 19 May, 2022) <https://quantumtechnologies.com/phishing-text-messages-rise/>

[33] Whispir, *SMS Phishing scams bite but businesses can make things right,* (Webpage, 15 March 2022) <https://www.whispir.com/en-au/blog/sms-phishing-scams-bite-but-businesses-can-make-things-right/>

[34] Atomic.io, It Wire, *Australians have lost trust in SMS, phone and email as scamming surges to record levels,* (Webpage, News Report, 21 March, 2024) <https://itwire.com/guest-articles/company-news/australians-have-lost-trust-in-sms,-phone-and-email-as-scamming-surges-to-record-levels.html>

[35] Ibid

**Figure 6: Trust index – Communications channels in Australia and New Zealand**




Source: *Atomic.io State of Digital Trust report, March 2024*

The cost-benefit analysis conducted by DAE estimated the extent of harm from these scams for 2023 at $56.4M each year. The analysis noted growth in SMS scams has been significant, with volumes increasing by 28% since 2021.

However, the CBA noted the introduction of the 2022 Scams Code may be contributing to a reduced impact of SMS scams with 2024 year-to-date financial losses down 57% compared to the same time last year.

# 2. What are the objectives, why is government intervention needed to achieve them, and how will success be measured?

The Australian Government is committed to the prevention of scam activity online, on telecommunications networks, and to strengthening the overall anti-scam framework to protect consumers.

The Government has determined that establishing and maintaining an SMS Sender ID Register will specifically target SMS impersonation scams, and lead to better outcomes for consumers and entities.

The implementation of the Register is intended to result in a measurable reduction in the prevalence of SMS Sender ID scams delivered on Australian telecommunication networks, and accordingly, reduced financial and other harms to consumers, and legitimate businesses. It is also expected to significantly restore consumer trust in SMS that utilise sender IDs.

## What are the objectives?

The objectives of an SMS Sender ID Register are to:

- decrease the frequency and impact (financial losses) of SMS impersonation scams on consumers
- increase protections for legitimate brands and agencies against bad actors impersonating them
- disrupt the business models for SMS impersonation scams
- restore public confidence in SMS as a communications channel; and
- ultimately, make Australia a harder target for scam activity.

Measurable success indicators of the new Register framework against the above objectives will include:

- a decrease in reported financial losses to Scamwatch for SMS scams (including SMS impersonation scams); and
- a decrease in reported SMS sender ID scams, as reported to Scamwatch.

Success indicators are dealt with in more detail in Chapter 7.

## Why is government intervention needed?

Impersonation scams delivered via SMS remain significant pain point for consumers. Strengthening and expanding provider requirements under a new Register framework will further enhance scam disruption efforts.

The need for policy intervention for SMS sender ID scams arises because there is no centralised, uniform approach to target this scam type. While some telecommunications providers have ad hoc arrangements with businesses, there is no uniform, holistic approach. As a consequence, the costs of these arrangements are borne by the entities targeted by bad actors and their telecommunications provider. In the majority of cases, where there are no such arrangements in place, the cost of these scams is borne by consumers.

Government intervention is required to significantly lessen the risk of Australians being harmed by sender ID impersonation SMS scams. The Register will operate as an additional safeguard by imposing a set of common measures on telco providers involved in sending SMS.

Based on overseas experience (refer section below), it is expected that the implementation of an SMS Sender ID Register will decrease the incidence of consumers receiving fraudulent messages via SMS. For businesses and Government agencies who are ‘spoofed’ by scammers via this contact method, the Register will enhance protection against damage to the reputation of their brands. An SMS Sender ID Register will also help to ensure that SMS remains a trusted channel of communication for brands and consumers alike.

The Government has determined that an operational SMS sender ID Register would serve to disrupt SMS as the key method by which scammers contact their would-be victims. The Register combined with strengthened rules for telcos involved in SMS traffic would also significantly expand protections available under the *Reducing scam calls and scam SMs C661:2022* Code. Without additional action, harms will further increase.

# Action taken to date

As the communications regulator, the ACMA has taken significant action to reduce scams over telecommunications networks. In relation to SMS scams, of particular note is the industry code*: Reducing scam calls and scam SMs C661: 2022* (the Code).

The first Reducing Scam Calls industry code was developed by Communications Alliance (CA), the peak body for the Australian telecommunications industry and Registered by the ACMA in December 2020.

In 2022 CA led the development of the new Reducing Scam Calls and Scam SMs industry code, which was Registered by the ACMA in July 2022. The revised Code added further tracing, and reporting measures, along with a new section dealing with the identification, tracing, and blocking of numbers associated with Scam SMS.

The code requires carriers and carriage service providers (telcos) to:

- identify and monitor for a range of characteristics that are common to scams, including calls and SMSs displaying calling line identification (CLI) from incorrect number ranges; high traffic volume and short duration calls
- ensure number integrity in calls and SMSs they are originating
- ensure Sender ID integrity in SMSs they are originating
- share information with other telcos and ACMA about scams
- trace the origin of scam calls and SMSs
- block the number associated with scam calls and SMSs; and
- seek assistance from international telcos.

The Code also requires telcos to make information available to their customers about current scams, how to report scams and how to avoid scams.

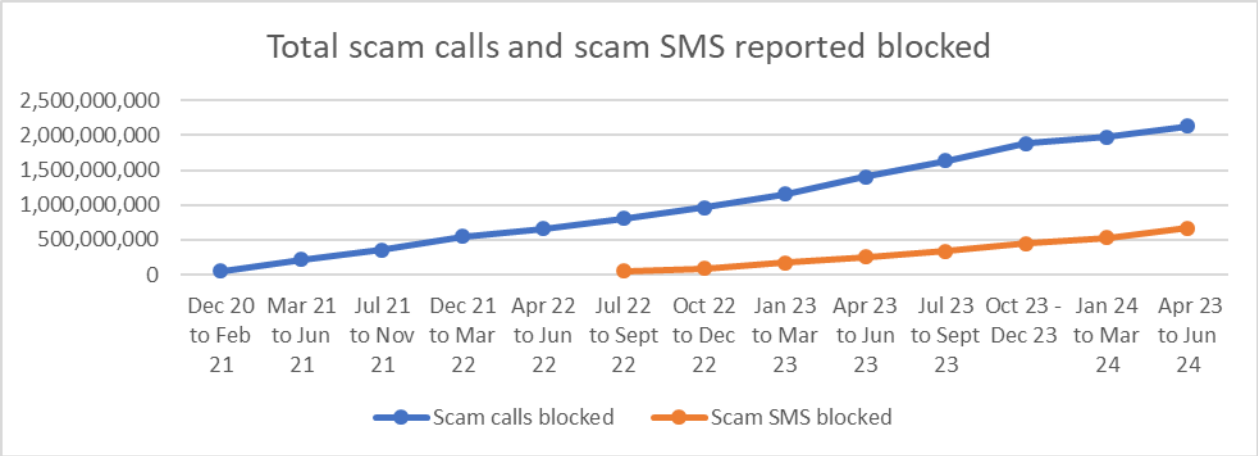
In addition to the Code, telcos are subject to other rules introduced by the ACMA to combat scams, including:

- identity verification processes before mobile numbers can be transferred between telcos via the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 – aimed at preventing harms caused by unauthorised porting of mobile phone numbers by malicious actors; and
- authentication processes for high-risk transactions via the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 – aimed at preventing malicious actors from gaining access to a person's personal information, business information or telco service.

# Blocking of scam SMSs

Up to 30 June 2024, telcos reported to the ACMA that over 2.1 billion scam calls have been blocked since December 2020, and more than 668.3 million scam SMS have been blocked since July 2022.

**Figure 7: Total Scam Calls and Scam SMS Reported Blocked**




Note: *This graphic shows the total scam calls/SMS blocked over time rather than aggregate scam calls/SMS blocked in each quarter - figures may fluctuate between quarters.*

Source: *ACMA; October 2024*

# Compliance action undertaken

The ACMA has actively monitored and enforced compliance with existing rules under the Code, and since 2022 has:

- Conducted 41 audits of individual telcos
- investigated 18 telcos; and
- Issued 15 telcos with directions to comply with the Code

Telecommunications providers who are found to be in breach of the code can be issued with a direction to comply in the first instance. This is the strongest enforcement outcome currently available to the ACMA for initial breaches of the code.

Once a telco is issued with a direction to comply, if future breaches are found, the ACMA may take stronger enforcement action such as commencing proceedings in the Federal Court. Telcos may face penalties of up to $250,000 for breaching ACMA directions to comply with the code.

Disrupting SMS impersonation scams has been listed as an ACMA compliance priority for 2024-25.

# SMS Sender ID Register pilot

On 15 December 2023, the ACMA commenced a voluntary pilot of the Register as an interim measure. The pilot initially involved the consolidation and centralisation of existing arrangements that certain entities had in place with their telco to protect their sender IDs from impersonation by scammers.

The pilot requires SMS that use a registered sender ID to only be sent by a single participating telco. If the sender ID and originating telco do not match, the message is blocked. Unregistered sender IDs are not impacted by the pilot.

The ACMA has been expanding the pilot by invitation, in order to manage growth in the pilot phase to make sure it works as intended. The focus has been on brands most at risk of impersonation and where SMS impersonation scams are causing the greatest detriment to consumers.

Lessons from the pilot (with particular regard to technical/operational issues) will assist to inform future operational aspects of the Register.

# Limitations of existing measures

## Operation of the Register pilot

The Register pilot in its current form is not scalable. The requirement to send SMS that use a registered sender ID through a single telco, limits participation as most entities use more than one telco to send SMS.

This has resulted in limited participation in the pilot, with fewer than ten entities currently taking part.

It is anticipated that the legislated Register will not be subject to the same limitations as the pilot – that is, it will not require traffic to originate from a single telecommunications provider.

## Need to establish an enforceable, industry-wide model

While there are some arrangements in place, including the pilot register, to control SMS Sender ID impersonation scams, there is no consistent or comprehensive approach.

While a number of providers have been proactive in working to prevent SMS scams, implementation of scam prevention processes and compliance with the Scams code is not consistent across all parts of the sector. The networked nature of telecommunications means that scam SMS usually travel across multiple networks owned by multiple telecommunications providers – both compliant and non-compliant – to reach their target.

For those in the industry, there are inherent challenges in identifying the origin of SMS traffic. Telecommunications providers have indicated that it can be difficult to know where an SMS had originated from when it was not sent directly from, for example, Telstra's network.[36]

There is also the issue of identifying all current providers of A2P messaging traffic (A2P messaging traffic, in general terms, refers to application to person messaging, where SMS are sent from a business application to mobile users via an automated process) While telecommunications carriers must hold a carrier licence, carriage service providers (including SMS aggregators) are not subject to any formal registration or licensing requirements, though they must comply with various laws and regulations.

A Register would result in a consistent, industry-wide approach in relation to SMS traffic with sender IDs. Both mandatory and voluntary registration models would include enforceable rules requiring telecommunications providers (including SMS aggregators) to check participating alphanumeric sender IDs to determine whether the sender was the registered party or agent.

## Overseas regulators recognise the need for intervention

A number of international jurisdictions have established SMS Sender ID registries. Methods used differ between countries but all have the shared goal of reducing the prevalence and often devastating impact of fraudulent SMS messages impersonating legitimate entities.

### Singapore

Singapore established a Register in March 2022 to enable organisations to protect their customers from receiving fraudulent SMS messages that spoofed the organisations' SMS sender IDs. Under the full mandatory regime which was announced in 2022, from 31 January 2023 onwards, all organisations intending to use alpha/numeric/alphanumeric sender IDs in their SMS messages to Singapore mobile users must first apply to participate and once approved, register the sender IDs via the portal.[37] Registered sender IDs will reach

---

[36] Charis Cheng, *This couple lost $98k in a sophisticated test message scam. Here's the one thing to look out for,* SBS News, (Published, 24 January, 2023) <https://www.sbs.com.au/news/article/a-melbourne-couple-lost-98k-in-a-sophisticated-text-message-scam-heres-what-they-warn-you-to-look-out-for/a0dcbrml3>

[37] Infocomm Media Development Authority (IMDA), Full SMS Sender ID Registration is to be required by January 2023, (Webpage, 17 October, 2022) <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2022/full-sms-sender-id-registration-to-be-required-by-january-2023>

Singapore users. All non-registered sender IDs are still delivered to users, but are marked as "Likely-SCAM".[38] Singapore has opted not to implement a complete blocking system, as this would adversely impact certain groups. A year after the introduction of the Register Singapore reported SMS scams had decreased by 64%.[39] The participation of SMS aggregators, implementing the register in stages and having a high adoption rate of SMS registrations have been important in facilitating the register's operation.

## Hong Kong

In Hong Kong the Office of Communications Authority (OFCA) initiated the SMS Registration Scheme in December 2023 to combat fraudulent SMS scam messages and provide greater consumer protection.[40] Business and industry with a practical need to send messages must apply to participate in the scheme. Once registered, organisations are able to send SMS messages using their registered sender IDs with the prefix #. All other SMS messages with sender IDs containing #, but not registered with the scheme are blocked by the telecommunications networks. The process makes it straightforward for the public to identify SMS messages received from a registered sender.

## UK, Ireland and Spain

The UK, Ireland and Spain have adopted voluntary registration, by checking whether the sender using that sender ID is the registered party. The Mobile Ecosystem Forum (MEF) operates the UK and Spanish systems. Initially introduced in the UK in 2018, the system successfully reduced the impersonation of alphanumeric message headers used by major UK brands.[41] The Register is designed to combat fraud and enhance the security of SMS communications. Organisations are able to register in order to protect their sender IDs. Once registered, a scammer's ability to use the same sender ID as a registered organisation or government department is limited. A blacklist has been established to block messages from sender IDs that have been used to send scam messages. DAE reported that the Irish Government has recently completed an assessment of future design of their SMS Sender ID Protection Registry, indicating an intention to move towards a mandatory registration scheme.[42]

## Finland

In November 2023, Finland introduced a voluntary sender ID Register, influenced by the systems in place in Singapore and the UK.[43] Users, who want to send alphanumeric messages, are required to register and following a three-month qualifying period, protection commences. The system allows approved organisations to register their brand name. The applicant is issued an SMS number beginning with 19, allowing identification in the SMS traffic of Finnish mobile networks but is not visible to the public.[44] The system began operating in February 2024 with approximately 70 registrations. Presently, there are 142 organisations registered with the

---

38 Singapore Network Information Centre (SGNIC), *Register Sender IDs early to avoid disruption to SMS communication with customers, (Webpage, 11 April, 2023)* <https://www.sgnic.sg/announcements/sgnic-news/announcement-details/2023/04/10/sender-ids-not-registered-with-the-ssir-will-be-blocked-after-six-months-transition-period-from-31-january-2023>

39 Infocomm Media Development Authority, *Enhanced measures against scam SM, (Webpage, 25 January, 2023)* https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2023/enhanced-measures-against-scam-sms#:~:text=Since%20the%20setting%20up%20of,down%20from%2010%25%20in%202021

40 The Government of Hong Kong Administrative Region, *SMS Sender Registration Scheme to be launched on December 28 to assist in combatting SMS scams,* (Webpage, Press Release, 20 December, 2023) <SMS Sender Registration Scheme to be launched on December 28 to assist in combating SMS scams (info.gov.hk)>

41 MEF Mobile Ecosystem Forum, *SMS Sender ID Protection Registry,* (Webpage accessed 14 March 2023) <https://mobileecosystemforum.com/sms-senderid-protection-registry/>

42 Originally operated by MEF as a voluntary system the Irish regulator is now working towards a mandatory system

43 YLE News, *Finland sets up ID system to thwart SMS scammers,* (Webpage, accessed 16 August, 2024) <https://yle.fi/a/74-20059967>

44 Traficom – traffic and communications services for you (Finland), *Protecting an SMS Sender ID,* (Webpage, Report accessed 20 August, 2024) <https://www.traficom.fi/sites/default/files/media/file/Guide%20on%20protecting%20an%20SMS%20Sender%20ID.pdf>

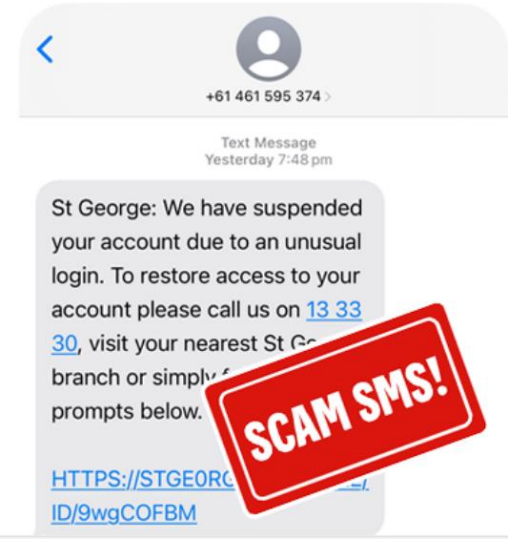
system.[45] Registration costs 200 euros per year.[46] SMS messages originating from any unauthorised parties using the protected SMS sender ID will not be delivered to Finnish mobile phone users, increasing both security and integrity. Messages sent from international gateways are blocked.

## Not a 'silver bullet' solution

It is expected that the implementation of the Register will reduce the incidence and impact of sender ID impersonation scams, and strengthen the ecosystem as a whole against SMS scam activity.

However, it is important to recognise the Register will not prevent all SMS scams, including SMS scams where the sender ID is a phone number and an entity is impersonated in the body of the SMS message. This is illustrated in Figure 8 below.

**Figure 8: SMS scam impersonating St George Bank in the body of the SMS message**




Source: *Latest Scams and alerts update, security centre | St.George Bank (stgeorge.com.au); accessed 6 November 2024*

Further, while implementing a Register is expected to significantly decrease the number and impact of SMS scam where entities are impersonated in an SMS message header, it is recognised that there is no single, 'silver bullet' solution. Scammers are agile and will invariably pivot to an alternative mechanism to defraud consumers. As SMS security comes under increased scrutiny, bad actors may shift to messaging apps such as WhatsApp or Viber.[47] The enabling legislation provides flexibility for the Register to include similar emerging technologies over time. That is, the legislation allows other kinds of communication services with message headers to be specified in the future as services which employ sender identifications. For example, rich communication services (RCS) which enable messaging either via Wi-Fi or an operator's cellular data connection, may be another such service specified in the future.

---

[45] Traficom, Registered SMS Sender ID users, (Webpage accessed 20 August, 2024) https://www.traficom.fi/fi/viestinta/laajakaista-ja-puhelin/rekisteroidyt-sms-sender-id-tunnukset?toggle=A%20-%20E&toggle=F%20-%20J&toggle=K%20-%20O&toggle=P%20-%20T&toggle=U%20-%20%C3%96

[46] Traficom – traffic and communications services for you (Finland), *Text message scams done by criminals are becoming more difficult – more than 70 sender IDs are already protected,* (Webpage, accessed 20 August, 2024) <https://www.traficom.fi/en/news/text-message-scams-done-criminals-are-becoming-more-difficult-more-70-sender-ids-are-already>

[47] The University of Sydney, *How can we stop scammers slipping fake texts into legitimate SMS threads?,* (Webpage, 23 March 2023) <How can we stop scammers sending SMS scams - The University of Sydney>

# 3. Policy options considered

The new Register framework will provide appropriate guardrails to reduce the frequency and impact of the SMS impersonation scam threat activity across multiple sectors of the Australian economy.

Having regard to SMS impersonation scam trends, approaches adopted overseas to combat these scams, and consultation undertaken to date, the Department has identified three options; two of which progress the establishment of a Register.

The Government has determined that a Register is an effective way to protect consumers from scams which impersonate alphanumeric sender IDs, and has allocated funding and introduced legislation to formalise the establishment of the Register. Two implementation options have been identified: registration can be voluntary (no obligation to register alphanumeric tags) or mandatory (alphanumeric tags must be registered if an entity wants to use or continue using alphanumeric tags and avoid messages either being blocked or flagged as possible scams).

Consistent with guidance from the Office of Impact Analysis, the Department has considered the option of retaining the status quo. Accordingly, for the purposes of this impact analysis, the three identified options are as follows:

- Option 1: status quo (no change)
- Option 2: voluntary registration of SMS sender IDs
- Option 3: mandatory registration of SMS sender IDs

## Option 1: Status quo (no change)

This option represents the status quo, as it is what would occur if no Government action is taken.

Under this option the ACMA would continue to monitor and enforce a telecommunications industry code requiring telcos to identify and block scam calls and SMSs. This is currently the Reducing Scam Calls and Scam SMs Code 2022 registered under the Telecommunications Act 1997. The Assistant Treasurer has introduced legislation to establish a Scams Prevention Framework that proposes overarching requirements to combat scams for designated industries and that the telecommunications scams code be made under the Competition and Consumer Act 2010.

This option would represent no change to current arrangements in relation to SMS sender IDs; that is, it is anticipated that:

- SMS messages with sender IDs would continue to be subject to impersonation by scammers – causing ongoing harm to consumers and to the reputation of retail brands and government entities
- confidence in SMS as a communications channel would be further diminished
- brands affected by scams could seek to make ad hoc arrangements with their telco to control the elements of scam blocking available to an individual telecommunications provider but there would be no centralised, consistent solution addressing these harms; and
- the volume of impersonation SMS sender ID scam messages received by citizens would likely continue.

This option is not recommended as the Government has formally committed to establishing and maintaining a national, centralised Register to combat SMS sender ID impersonation scams; and in doing so, has:

- allocated specific funding to the ACMA to establish and maintain an SMS Sender ID Register, and

- introduced the Telecommunications Amendment (SMS Sender ID Register) Act 2024 which creates a legislative basis for the ACMA to establish and maintain the Register.

Maintaining the status quo would be contradictory to these measures.

In addition, this option does not contribute to the objectives of an SMS Sender ID Register; namely, to:

- decrease the frequency and impact of SMS impersonation scams on consumers
- increase protections for legitimate brands and agencies against bad actors impersonating them
- disrupt the business models for SMS impersonation scams
- restore public confidence in SMS as a communications channel; and
- ultimately, make Australia a harder target for scam activity.

A key consequence of maintaining the status quo is the likelihood of future harm to individual consumers and legitimate entities resulting from continuing SMS sender ID scams. In the cost-benefit analysis conducted, harms emanating from SMS sender ID scams were estimated at $26.6 million across approximately 108,000 scams in 2023. These scams can cause significant stress for scammed consumers, in addition to wasted time attempting to resolve issues related to being scammed. Businesses that are impersonated via these scams spend time resolving customer issues related to being scammed. Further explanation of identified harms is discussed at Chapter 4.

While the status quo is not considered an appropriate option for the reasons outlined above, it has been used for the purposes of calculating anticipated costs and benefits of each option; that is, this option is used as a 'base case' to measure option 2 (voluntary registration) and option 3 (mandatory registration). These costs and benefits are explored in Chapter 4.

# Option 2: Voluntary registration of SMS sender IDs

Under this option, registration of SMS sender IDs would occur on a voluntary basis, where interested entities would be able to register alphanumeric sender IDs.

If the sender ID is registered but the sender is not the registered party, the SMS would be either blocked or flagged as possible scams. Unregistered sender IDs would not be blocked or tagged, and could still be used for scams.

The Register would only be used by willing entities prepared to participate on a 'user pays' basis.

Under this model, a separate 'blocklist' can be maintained, where variations of registered sender IDs (e.g. Auspost instead of AusPost) are also blocked.

Under a voluntary registration model, new rules would be introduced which apply to telecommunications providers sending SMS with alphanumeric sender IDs. These rules would be enforced by the ACMA.

## Advantages and disadvantages of voluntary registration

### Advantages:

- ✓ Entities can choose whether or not to register their alphanumeric sender IDs. If they choose not to register, they can continue to use their alphanumeric sender IDs as usual and will not incur register related costs.
- ✓ Registered alphanumeric sender IDs are protected.
- ✓ If the sender ID is registered and the sender does not have a valid use case, or the sender was not the registered party for that sender ID, telecommunications providers would block or tag the SMS as a possible scam.

### Disadvantages:

- A voluntary Register would provide less comprehensive protection to consumers as scammers would be able to sequentially target entities and brands that have not registered. Voluntary registration would not stop criminals targeting businesses and entities who have not registered alphanumeric sender IDs. Consequently, members of the public would likely continue to receive scam SMS impersonating brands that have not registered.
- Consumers 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 with alphanumeric sender IDs.
- A blocklist is needed to prevent variations of legitimate alphanumeric sender IDs being used by scammers. This is usually a manual process which involves adding new variations to an ever increasing blocklist that can be difficult to maintain. Consumers will continue to receive scams via these variations until they are added to the blocklist.
- As with mandatory registration, there would be costs to businesses and entities who choose to register.

# Option 3: Mandatory registration of SMS sender IDs

Under this option, all brands and entities wishing to send SMS with alphanumeric sender IDs would be required to register these as sender IDs. Sender IDs that are not registered would either be blocked, or tagged as possible scams.

Telcos involved in sending SMS with alphanumeric sender IDs would be subject to enforceable rules and prohibited from sending SMS with alphanumeric tags unless the tag is registered and the messages originate from a legitimate sender. SMS with unregistered sender IDs would be blocked or tagged as possible scams.

It is important to note that under a mandatory Register scheme, businesses and entities wishing to send SMS to end users would still able to use mobile numbers as sender IDs.

## Advantages and disadvantages of mandatory registration

### Advantages:

- ✓ Provides a very high level of protection to brands and consumers, as SMS traffic with alphanumeric sender IDs will only reach consumers where the sender ID is registered and originates from a legitimate sender. All other SMS with alphanumeric sender IDs will be blocked or tagged as possible scams, giving consumers confidence that SMS which appear in existing message streams are legitimate.
- ✓ There is therefore no need to also maintain a blocklist.
- ✓ Scammers would not be able to target consumers via use of alphanumeric sender IDs that have not been registered.

### Disadvantages:

- Mandatory registration would mean all entities and brands who wish to continue using alphanumeric sender IDs for SMS would have to register them to avoid messages either being blocked or flagged as possible scams, and would incur fees for registration.
- This means that entities who are not impacted by scams would either have to stop using their alphanumeric sender IDs (and use a mobile number or short code instead), or register and pay to keep using them. (Should the sender ID user keep trying to use the alphanumeric tag, they would need to accept their messages will be overstamped as possible scams or blocked).
- Legitimate SMS could be blocked or tagged as possible scam if an entity has not registered its alphanumeric sender ID by the date the Register comes into full effect.

# 4. What is the likely net benefit of each option?

In line with OIA requirements, a regulatory burden estimate has been completed for each viable option.

The assessment of costs and net benefits has been informed by a cost-benefit analysis (**CBA**) of mandatory and voluntary registration options for establishing the SMS Sender ID Register conducted by Deloitte Access Economics (**DAE**). A copy of the full CBA is available at **Appendix A.**

The CBA considers the likely costs to industry and government of implementing, integrating and maintaining the Register, and to sender ID users to undertake registration and renewal activities. The likely benefits accrue to sender ID users and consumers from avoided SMS sender ID scams. Costs and benefits are assessed over a 10-year period, relative to a base case in which the Register is not established (the status quo), and assessed across:

- government
- telecommunications industry participants
- sender ID users (organisations and entities using or likely to use sender IDs); and
- consumers.

## Data collection

To capture necessary data to inform the modelling inputs for both costs and benefits, primary and secondary data collection methods were utilised by DAE.

### Primary data collection

Surveys were developed and distributed to businesses and consumers. The surveys received a total of 618 responses from organisations (including 151 sender ID users) and 1,011 responses from Australian consumers.

The organisation survey is not representative of the population of businesses with the sampling approach targeting consumer-facing businesses and those likely to be using sender IDs.

The key inputs collected from the organisation survey, which informed modelling included:

- the use of sender IDs across business (including the number of sender IDs used)
- impact of sender IDs on consumer engagement
- actions taken because of the proliferation of SMS scams
- responses to voluntary and mandatory registration schemes; and
- 'Willingness to pay' for registration under voluntary and mandatory registration schemes.

The consumer survey respondents comprised a broadly representative sample across gender, age and location.

The key inputs collected from the consumer survey which informed modelling include:

- the proportion of SMS scams utilising sender IDs
- the rate of reporting to Scamwatch
- the proportion of consumers attempting to resolve issues related to being scammed
- time spent attempting to resolve issues related to being scammed
- the impact of SMS scams on consumer engagement with legitimate communications and the level of trust in SMS as a platform; and
- perspectives on the impact that the introduction of a Register would have on trust in SMS.

Targeted consultations with telecommunications industry participants, high volume sender ID users from business and government and overseas regulators were also undertaken to validate assumptions and better

understand the potential impacts. The consultations were supported and informed by prior submissions and survey results collected by the Department, as well as qualitative findings from the pilot.

Further information on the surveys and consultations is detailed in DAE's report at **Appendix A**.

## Secondary data collection

A literature review was undertaken on the potential costs and benefits of mandatory and voluntary registration schemes. Documentation and findings from overseas jurisdictions who have, or are in the process of, implementing comparable Registers served to inform the potential impact of a Register in Australia.

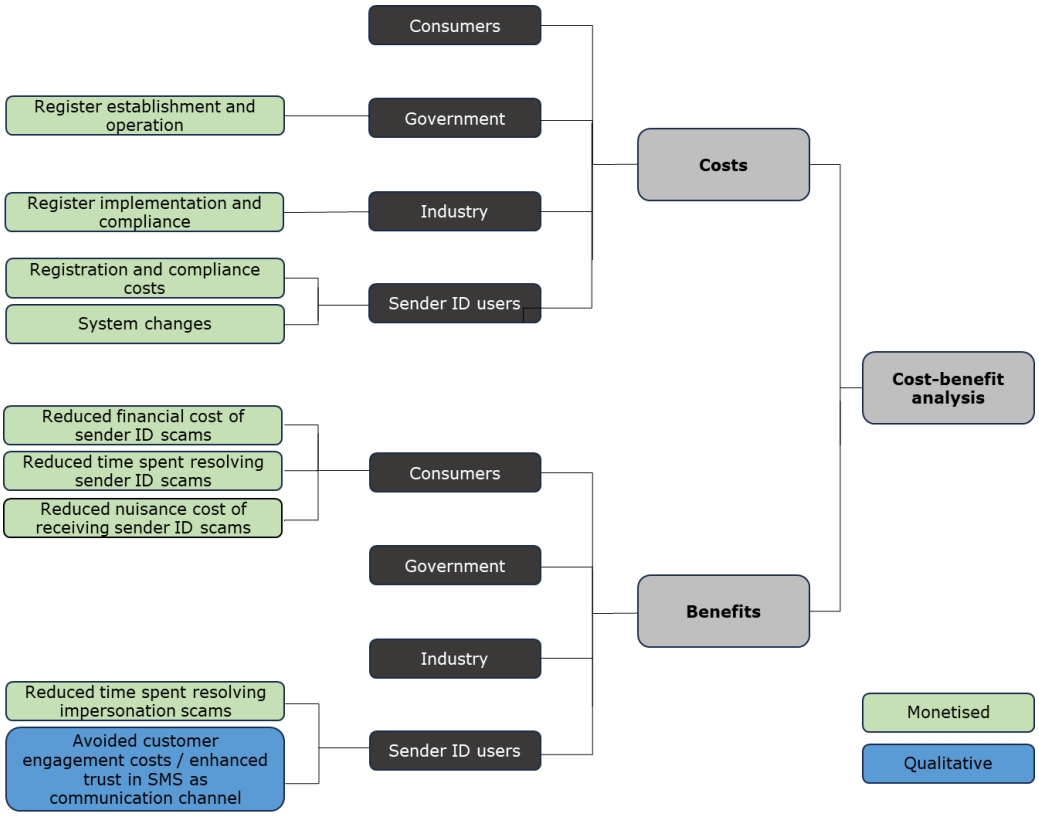
Data on the number, characteristics and average losses from SMS scams were primarily informed from Scamwatch public data.

# Methodology

DAE's modelling technique monetises costs incurred, and benefits gained across stakeholder groups to monetary values, which allows for the weighting of costs of performing certain actions against the benefits. The CBA weighs the costs of the two SMS Sender ID registration scheme options (voluntary registration and mandatory registration) against the benefits the schemes create.

Figure 9 provides a conceptual overview of the model structure that was used to define the categories of cost and benefit inputs for the CBA.

**Figure 9: Model structure to define categories of costs and benefits inputs for the CBA**




Source: *Deloitte Access Economics 2024*

The CBA relied on the monetised values of the estimated costs and benefits, gathered through the consumer survey, organisation survey, secondary data and stakeholder consultation.

While the primary data collection methods used supported analysis of costs and benefits in the CBA, there are limitations with the data due to the nature of utilising paid panels to collect data. There may exist an incentive for some participants to answer as quickly as possible or to not answer honestly. To address these potential issues the survey provider undertook several validation processes, detailed in page 17 of the CBA.[48]

## Cost inputs

Key costs relate to the cost of implementing, maintaining and interfacing with the technical components of the Register. For government, it is assumed that the budget allocation appropriated in 2023-24 Budget to establish and maintain the Register reflects the extent of relevant costs. For telecommunication industry participants, the scale of costs has been sourced through targeted consultation.

Sender ID costs scale linearly with the number of sender ID users that are expected to register. While estimates of current usage have been sourced from consultations with industry and through the organisation survey, the expected number of sender IDs registered under either option remains highly uncertain. As such, sensitivity and break-even analysis was undertaken on these inputs.

## Benefit inputs

Benefits relate to direct and indirect costs that are avoided due to a reduction in sender ID scams. The key assumptions that drive benefits include the decrease in total sender ID scams under each policy option and how quickly scammers shift to other types of communication methods to conduct scams.

The benefits assessed for consumers are: reduced financial cost of sender ID scams, reduced time spent resolving sender ID scams and reduced nuisance cost of sender ID scams.

## Timeframe

The analysis considers the period from 2024-25 to 2034-35. As per the OIA's guidance, a timeframe of 10 years is utilised as the default period of analysis. The analysis considers the time required to establish the Register (which is expected to be operationalised by the end of 2025) and its ongoing operation across the remaining period of the 10-year timeframe.

# Option 1: Status quo (no change)

Under this option, no Register would be implemented, and the costs to the economy emanating from SMS sender ID impersonation scams would continue. No benefits have been quantified for this option.

## Costs

### Sender ID users and consumers

For the purposes of this Impact Analysis, DAE estimated the current level of harm (costs to sender ID users and consumers) associated with sender ID impersonation scams below; these values reflect the extent of harm in 2023.

---

[48] Additionally, to appropriately use the observed data sets, the use of medians has been applied where appropriate to manage the skewed distribution of results.

**Table 3: Total monetised harm associated with sender ID impersonation scams.**

| Harm | Annual Harms 2023 ($ million) |
|---|---|
| Financial cost of sender ID scams | 26.6 |
| Time cost of sender ID scams | 11.0 |
| Nuisance cost of receiving sender ID scams | 3.9 |
| Avoided business impersonation costs | 14.9 |
| **Total harm (annual)** | **56.4** |

Source: *Deloitte Access Economics (2024).* Note: figures may not sum due to rounding

The trajectory of sender ID scams under the base case (the status quo) will therefore determine the potential level of annual harm in future years. In recent years, growth in SMS scams has been significant; between 2021 and 2023 Scamwatch reported a 63% increase in the number of reports received regarding SMS scams. However, the introduction of the Scams Code may be contributing to a reduced impact of SMS scams with 2024 year-to-date[49] financial losses from SMS scams down 59% compared to the same period last year. While recent figures may suggest the volume of SMS scams is declining, and this may be in part a result of other interventions, there is a high degree of uncertainty around the future trajectory, the share of harms that may be associated with sender IDs and the extent to which any reduction can be attributed to other interventions. The CBA assumes a modest 5% annual growth in the volume of scams under the base case, (noting that a sensitivity analysis has been conducted – refer **Appendix A**).

### Telecommunications industry participants

Under this option, telecommunications industry participants would not incur costs to integrate with the Register, or comply with Register rules.

### Government

Under this option, no additional costs would apply; noting Government costs from the 2023-24 Commonwealth Budget have already been appropriated to the ACMA.

# Option 2: Voluntary registration of SMS sender IDs

## Costs

This section outlines the costs faced by stakeholders under a voluntary registration scheme. Costs are incurred in the financial years indicated or when the Register establishment activities are anticipated by the ACMA to occur. Specifically:

- technical costs related to telecommunication industry participants integrating with the government-run Register occur by the end of 2025 (financial year 2025-26); and
- sender ID user costs are assumed to commence from financial year 2025-26.

---

[49] January to August

## Government

Government costs are sourced from the 2023-24 Commonwealth Budget. The funding has already been appropriated to the ACMA and is considered to not materially differ between policy options.

This reflects that the expected technical design of the Register would be comparable across both options. However, under a voluntary registration scheme there is an expectation that government would administer a block list of sender IDs closely related to those already registered, as currently happens under the UK model. Based on the experiences of telecommunications companies currently undertaking similar activities for customers, a block list has the potential to become a time-consuming activity to prepare and maintain as scammers iterate through the infinite available variations.

**Table 4: Australian Government 2023-24 Budget allocation for SMS Sender ID Register.**

| | 2025* | 2026 | 2027 | Ongoing |
|---|---|---|---|---|
| Budget allocation ($ million) | 6.3 | 2.1 | 2.1 | 2.2 |

*Captures both the 2024 and 2025 budget allocation

Source: *Deloitte Access Economics (2024)*

## Telecommunications industry participants

Telecommunications industry participants are expected to incur an initial cost upon the creation of the Register and smaller ongoing costs to maintain their systems' integration with the Register.

These costs are incurred by the mobile network operators 'MNOs' as well as SMS aggregators who may participate in the Register. SMS aggregators are the gateway between businesses and mobile network operators. Australian businesses can use a messaging gateway to send bulk SMS messages for alerts, marketing and communication campaigns or 2-way messages via a gateway network.

Noting that any telcos in the SMS supply chain could incur costs, the CBA has used the figure of 30 as the number of SMS aggregators[50] assumed to incur costs, which is the estimated number of Tier 1[51] aggregators (those who connect directly with an MNO).

The CBA has adopted a conservative approach and recognises the possibility of increased costs once the Register is implemented – while a small amount of costs were allocated to aggregators, these were allocated to those large and medium sized aggregators with an expected high volume of SMS sender IDs. (DAE consultations with aggregators also highlighted the significant market share held by large sized aggregators).

The initial costs are expected to include any technical changes required as well as any assistance that A2P SMS customers may require through the registration process (noting that sender ID users would register with the ACMA or a contracted Register administrator).

The MNOs consulted for the CBA were asked to estimate these costs and advised that they currently undertake many business processes to prevent scam SMS being sent, and that they would not expect the Register to involve substantial incremental costs. MNOs were unable to provide precise estimates of any incremental costs given the uncertainty regarding the technical design of the Register.

---

50 The use of 30 aggregators is based on the approximate number of large and medium sized aggregators referenced in the *Reducing the impact of scams delivered via short message service (SMS) Regulation Impact Statement* prepared by the ACMA in 2022

51 In general terms, tier 1 aggregators connect directly with mobile network operators and tier 2 aggregators do not connect directly to mobile network operators.

Some stakeholders also stressed the importance of a phased implementation to avoid a high volume of initial registrations concentrated in a short period of time. Despite the uncertainties, stakeholders did not reflect a view that there are likely to be material differences in costs across voluntary and mandatory registration.

To provide an indicative estimate of the feasible incremental costs to MNOs, the CBA used estimated costs from the Irish regulator, ComReg, from an equivalent Register in Ireland (adjusted for exchange rates).

**Table 5: Indicative telecommunication industry participants costs.**

| | Number | Initial | Ongoing (annual) |
|---|---|---|---|
| Mobile network operators | 3 | $250,000 | $33,000 |
| SMS aggregators | 30 | $250,000 | $33,000 |

Source: *Deloitte Access Economics (2024)*

## Sender ID users

Estimates of costs for sender ID users captures both the compliance costs considered in the CBA and registration and fees. While a decision on cost recovery arrangements has yet to be made, it is understood that brands and entities participating in the Register will be charged fees to recover government costs of operating the Register.

In line with this understanding, the fee burden on sender ID users is estimated to be equivalent to the government costs included in the CBA.

Anticipated user registration rates: voluntary registration

An estimated 300,000 sender IDs are currently utilised in Australia, capturing a broad range of users from government departments, large business, sole traders, community organisations and individuals.

To capture potential differences in registration rates, costs faced and benefit accumulation, sender ID users have been segmented into three categories broadly based on the complexity of their operations. The segmentation has been informed by inputs from telecommunications industry participants on the use of sender IDs across groups and findings from the organisation survey on the average number of sender IDs used. The segments cover:

- **High volume users:** 500 trusted brands and government entities that use a larger number of sender IDs as a key part of the business-as-usual activities.
- **Medium volume users:** 22,000 business and other organisations who regularly utilised a small number of sender IDs
- **Low volume users**: 240,000 organisations/individuals who likely utilise a single sender ID.

Registration intentions were estimated through DAE's organisation survey by asking respondents whether they would register under each policy option.

The results find similar rates of registration among current sender ID users with **75%** indicating they would register under a voluntary registration scheme. While the survey results indicated similar registration levels, there can often be response bias based on positive or negative associations with terminology (e.g. voluntary versus mandatory) and in the sequencing of responses (i.e. response anchoring to an initial question). To manage the risk of bias and potential uncertainty of inputs, a sensitivity analysis has been conducted on the percentage of business registrations.

The key driver of cost between the options considered is how many of the existing sender IDs are likely to be registered under a mandatory or voluntary registration scheme. Under each option, users wishing to register their sender IDs would be required to apply to become an approved user before registering their sender ID(s).

Costs have been separately calculated for the three user segments, with the high-volume users assumed to incur a system change cost to integrate new business processes and/or technical requirements.

This assumption has been based on stakeholder consultation conducted by DAE; it is understood that there can be significantly different business practices with sender IDs depending on the size and industry of the business. Stakeholders highlighted that high-volume users (typically large businesses) would be more likely to have a range of different integrated systems that may need updates to comply with sender ID registration. In contrast, medium and low volume users are less likely to have these integrated systems in place (with some businesses expected to have fully outsourced their system arrangements) and would therefore not incur system change costs.

The estimated per user cost of registration is outlined below.

**Table 6: Sender ID user costs of registration.**

| | System change costs | Administrative cost (initial) | Administrative costs (renewal) |
|---|---|---|---|
| High volume | $5,000 | $213 | $128 |
| Medium volume | - | $213 | $128 |
| Low volume | - | $213 | $128 |

*Source: Deloitte Access Economics (2024)*

Based on anticipated user registration rates, the total cost (in terms of system change costs and administrative costs to register) for **Option 2 voluntary registration** is outlined below. Of note is that the small per user administrative cost of registration and renewal spread across many users is the key driver of cost. Registration rates that significantly differ would materially impact the overall cost of registration.

**Table 7: Sender ID user costs: voluntary registration.**

| Type of cost | Cost ($ million) |
|---|---|
| System change costs | 1.9 |
| Administrative cost, initial | 29.1 |
| Administrative cost, renewal | 17.5 |

Source: *Deloitte Access Economics (2024)*

Sender ID costs have been calculated based on the estimated population of sender ID users by user size (high, medium, low). The registration rate is different for low volume users (50% registration) compared with medium and high-volume potential registrants (expected 78% registration rate).

The CBA found that low volume potential registrants constitute the highest volume of users (240,000). This is detailed in table 3.3 of the CBA.

## Consumers

Consumers are not expected to face any direct costs under this option. The CBA noted that while it is possible consumers could experience indirect costs because of telecommunication providers passing on compliance costs, these costs could also be passed on through the A2P SMS supply chain or to sender ID users.

## Benefits

The benefits modelled in the CBA represent financial and non-financial benefits that accrue to consumers and sender ID users.

### Consumers

Consumers benefit under this option due to the reduced financial and non-financial costs of being scammed through SMS impersonation scams using sender IDs. This includes avoided money lost to scammers and reduced time spent resolving issues related to being scammed. As identified in Option 1 (status quo), the total monetised harm associated with sender ID impersonation scams was calculated by DAE at **$56.4 million** for 2023. Each of the consumer harms monetised as part of that calculation are explored below.

A. Financial cost of SMS sender ID scams to consumers

Financial losses for consumers from sender ID scams are the largest individual harm.

Scamwatch reported 110,000 SMS scams corresponding to approximately $26.9 million in financial losses in 2023. Further, between the period of 1 January and 31 July 2024, Scamwatch received 63,121 reports where the scam contact mode was listed as 'text message' (SMS). Of those, 50,062 reported scams involved 'impersonation'. Changes to the Scamwatch form incorporating a specific data field relating to sender IDs went live in September 2024. Early data provided by NASC for the period from the 6th to the 30th September, since the commencement of the new data field, reported 126 scam messages where the impersonation occurred in the sender ID. Refer to Chapter 7 for further information.

To estimate the number and financial cost of sender ID scams specifically, DAE's consumer survey asked scammed respondents to report characteristics of SMS scams they received. The survey found:

- sender ID impersonation scams are prevalent, accounting for 55% of all SMS scams received and 37% of all SMS impersonations scams that resulted in a financial loss; and
- there were mixed views from industry stakeholders on the prevalence and associated financial costs of sender ID scams. Although these scams may represent only a sub-set of SMS scams, there was a view by some consulted that the ability of sender ID scams to impersonate legitimate organisations more effectively or embed themselves into existing message threads means they pose a greater potential risk to consumers.

The financial cost of sender ID scams is based on the average financial loss of SMS scams reported by Scamwatch in 2023 ($246). However, this may be a conservative approach with DAE's consumer survey finding that the average reported financial loss of a sender ID scam ($278) is 12% higher than other types of SMS scams ($248). Additionally, the average financial loss masks significant variance in consumers' individual experiences, with the median loss to an SMS phishing scam in 2023 amounting to $2,012 while the median loss to an investment scam initiated via SMS was $14,400.Scams reported to Scamwatch only represent a fraction of scams, suggesting the reported financial losses reflect a lower bound estimate.[52] To account for unreported scams, DAE's consumer survey asked consumers whether they reported a scam to Scamwatch. The results find that 70% of consumers experiencing financial losses from SMS scams did not report the scam. Additionally, the reported financial losses between reported and non-reported scams did not differ materially ($248 versus $227).

---

[52] Australian Competition and Consumer Commission, *Targeting Scams: Report of the National Anti-Scam Centre on Scams Activity 2022* (Report, April 2023) <https://www.scamwatch.gov.au/system/files/Targeting-scams-report-2023_0.pdf>.

Based on the parameters discussed above, DAE's CBA model estimates that the **total financial losses** related to SMS sender ID scams in 2023 was **$26.6 million across approximately 108,000 scams**. This is detailed in the table below.

**Table 8: 2023 Financial losses from sender ID impersonation scams.**

| Description of input | Unit | Value | Source |
|---|---|---|---|
| Number of SMS scams reported to Scamwatch | # | 109,615 | Scamwatch |
| Proportion of SMS scams that are not reported to Scamwatch | % | 70 | ACCC & Consumer Survey |
| Proportion of SMS scams related to impersonation | % | 80 | ACCC |
| Proportion of SMS impersonation scams utilising alphanumeric sender IDs | % | 37 | Consumer survey |
| Average financial cost of SMS scams | $/scam | 246 | Scamwatch |
| Number of alphanumeric sender ID scams | # | 108,153 | Calculation |
| Cost of alphanumeric sender ID scams | $ | 26,605,753 | Calculation |

Source: *Deloitte Access Economics (2024)*

B. Consumer time spent resolving SMS sender ID scams

In addition to financial costs associated with scams, consumers face costs (in terms of time spent) related to resolving issues such as attempting to recover financial losses, changing passwords and regaining access to online accounts. These issues are common with **85%** of consumers being scammed via SMS reporting that they encounter these additional non-financial issues. Issues flowing from scams have a material cost with the vast majority (78%) of scam victims spending an average of 3.5 hours attempting to resolve them.

DAE has commented this is likely a conservative estimate with over half of consumers spending more than the maximum amount of time listed in the survey (more than 5 hours) resolving issues.

Applying the OIA guidance on value of leisure time ($37.00 per hour) to these estimates suggests that the time cost imposed on consumers by sender ID scams in 2023 was **$11.0 million across approximately 108,000 scams**[53]. This calculation is detailed in the table below.

**Table 9: Time spent resolving sender ID scams.**

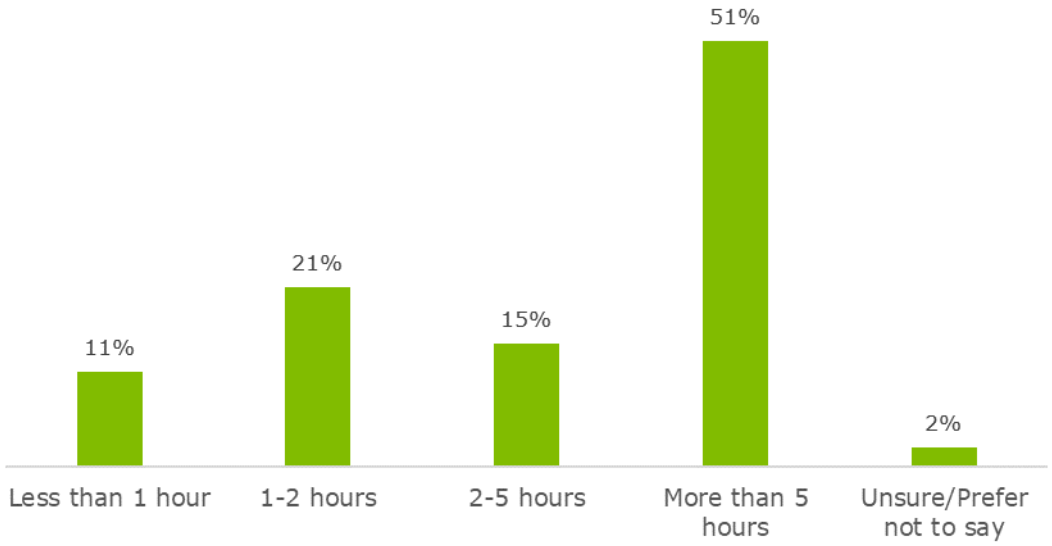
| Description of input | Unit | Value | Source |
|---|---|---|---|
| Number of alphanumeric sender ID scams | # | 108,153 | Calculation |
| Proportion of consumers attempting to resolve issues related to being scammed | % | 78 | Consumer survey |
| Average time spent resolving issues related to being scammed | Hours | 3.5 | Consumer survey |
| Value of leisure (median wage) | $/hour | 37 | OIA |
| **Time cost of alphanumeric sender ID scams** | **$** | **10,924,582** | **Calculation** |

---

[53] Office of Impact Analysis (OIA) Regulatory Burden Measurement Framework, Department of the Prime Minister and Cabinet (2024).

Source: *Deloitte Access Economics consumer survey (2024)*

**Figure 10: Responses to the Question: How much time did you spend trying to resolve issues caused by the scam SMS?**




Source: *Deloitte Access Economics consumer survey (2024)*

C. Nuisance cost of receiving sender ID scams

The high volume of SMS scam communications imposes a nuisance cost on consumers by wasting their time, requiring them to discern if a message is legitimate and degrading their experience of SMS as a communication platform. DAE's consumer survey found this impact is material with 82% of consumers reporting they find SMS scams to be a waste of time and 26% report them to be confusing.

Although this harm is intangible, this was estimated by DAE based on consumer's willingness-to-pay (WTP) to not receive SMS scams by work commissioned by ComReg in Ireland. This analysis undertook WTP experiments to elicit the value consumers place on being free from SMS scams[54].

The study utilised several variations with different payment vehicles producing annual WTP values between AUD $12 and $195. These values are produced based on the responses from consumers who have not been scammed to isolate the harm associated with nuisance from financial loss.

Applying the above WTP values to the population of Australian mobile phone users who received SMS scams multiple times per week (30%) and the share of SMS scams associated with sender IDs (55%) implies a total nuisance cost of sender ID scams at between $39 million and $633 million annually[55]. This is calculated in the table below.

---

[54] Europe Economics (2023) Scam calls and texts in Ireland – costs and benefits of interventions <https://www.comreg.ie/media/2023/06/ComReg-2352a.pdf>.

[55] Australian Competition and Consumer Commission, *Targeting Scams: Report of the National Anti-Scam Centre on Scams Activity 2022* (Scamwatch Report, April 2023) < https://www.nasc.gov.au/system/files/Targeting%20scams%202022.pdf 2022.pdf>.

**Table 10: Nuisance cost of alphanumeric sender ID scams.**

| Description of input | Unit | Value | Source |
|---|---|---|---|
| Adult population (15+) with mobile phones | # | 19,686,493 | ABS |
| Proportion of people receiving SMS scams more than once a week | % | 30 | ACMA |
| WTP to avoid receiving SMS scams | $ | 12.00 | ComReg |
| Proportion of SMS scams messages received using alphanumeric sender IDs | % | 55 | Consumer survey |
| Adjustment for only reducing SMS scams by approximately half | % | 10 | Assumption |
| Time cost of alphanumeric sender ID scams | $ | 3,897,926 | Calculation |

Source: *Deloitte Access Economics (2024)*

However, the potential avoidable harm is likely less as the WTP parameters capture the value of receiving no scam SMS rather than a 55% reduction. As such, a conservative 10% assumption was applied to the lower bound to capture the potential avoidable nuisance harm associated with sender ID scams ($3.9 million).

## Sender ID users

SMS impersonation scams impose costs on legitimate organisations and entities because consumers contact these organisations to resolve issues such as recouping money, safeguarding data or recovering access to online/bank accounts.

DAE's consumer survey suggests that those consumers who experienced a sender ID scam spent at least 295,000 hours in 2023 attempting to resolve issues related to being scammed. It follows that at least some of this time would impose a corresponding burden on organisations and entities (sender ID users).

To estimate the cost imposed on impersonated organisations, DAE's organisation survey ascertained the share of sender ID users that were aware of having their sender IDs impersonated (31%), and the average amount of time spent resolving customer complaints related to the SMS impersonation scam (25 hours). DAE estimated as many as 250,000 organisations are currently using sender IDs, and it is assumed that those experiencing impersonation are concentrated among large and trusted brands. This assumption is based on stakeholder input that most sender IDs are used by small businesses or low volume users at little risk of being impersonated.

Based on these inputs, Australian organisations spend approximately 174,000 hours responding to consumer issues related to sender ID impersonation scams, amounting to a time cost of **$14.9 million in 2023[56].**

---

[56] The total calculated cost is $14,851,955 (rounded to $14.9 million in the body of the CBA).

**Table 11: Time spend resolving customer complaints.**

| Description of input | Unit | Value | Source |
|---|---|---|---|
| Number of organisations using sender IDs | # | 22,500 | Assumption |
| Proportion of sender ID users receiving impersonation complaints from consumers | % | 31 | Business survey |
| Time spent resolving impersonation issues from customers | % | 25 | Business survey |
| Hourly wage | $ | 48.67 | OIA |
| On-costs | % | 175 | OIA |
| Annual cost of customer complaints | $ | 14,851,955 | Calculation |

Source: *Deloitte Access Economics (2024)*

While these costs account for the impact of impersonation related complaints for sender ID users, stakeholders consulted suggested that scammed consumers will also engage with their bank to attempt to reverse payments or receive compensation. DAE's consumer survey validates this view: two-thirds (65%) of scammed consumers reported the scam to their bank. As such, the estimated harm of consumers engaging with impersonated organisations is likely a lower-bound estimate, as banks are also likely to incur time and material costs to manage customer issues associated with compromised bank accounts or card details to determine if any action can be taken to recover lost funds.

### Regulatory burden estimate

In line with OIA requirements, a regulatory burden estimate must be completed for each viable option. Based on the CBA, the average annual regulatory cost is outlined below.

The estimate of costs to sender ID users captures both the compliance costs considered in the CBA and registration and fees. While a decision on cost recovery arrangements has yet to be made, it is understood that brands and entities participating in the Register will be charged fees to recover government costs of operating the Register. In line with this expectation, the fee burden on sender ID users is estimated to be equivalent to the government costs included in the CBA.

**Table 12: Average annual regulatory costs (from businesses as usual), undiscounted over 10 years.**

| Change in costs ($ million) | Industry | Sender ID users | Consumers | Total change in cost |
|---|---|---|---|---|
| Voluntary registration | 1.7 | 19.7 | - | 21.4 |

Source: *Deloitte Access Economics analysis (2024)*

## Total benefits – voluntary registration

The level of protection under the voluntary registration option is considered less than under the mandatory registration scheme, as scammers could still use closely related but unregistered sender IDs that could, in practice, impersonate legitimate organisations or create a compelling scam lure.

### Adjustment to benefits calculation for the CBA

It was assumed for the purposes of the CBA, that the voluntary registration scheme would be 80% as effective as the mandatory registration scheme, resulting in a 20% adjustment to benefits.

The 20% adjustment is an assumption utilised as an input to the CBA to reflect the expected lower efficacy of the voluntary registration model relative to the mandatory registration model.

This is based on, among other things, advice from stakeholders consulted during the CBA, and available literature on overseas registers which highlighted the potential limited benefits of voluntary registration relative to the mandatory registration option. However, as the practical difference in efficacy between the two options within the Australian context is unknown, the assumed 20% benefit adjustment was used.

This adjustment may be conservative as engagement with overseas regulators operating similar registers reported limited benefits associated with a voluntary registration approach. (In practice, the reduction in benefits by 20% could potentially be much larger, and according to some stakeholder feedback, the voluntary model may not be effective in addressing SMS sender ID impersonation scams at all.)

**Table 13: Total benefits for voluntary registration, NPV over 10 years at a 7% discount rate.**

| Harm | Voluntary registration |
|---|---|
| Effectiveness rate | 75% |
| Annual benefit decrease | 5 percentage points |
| Option effectiveness adjustment | -20% |
| Avoided financial cost on scams ($ million) | 89.1 |
| Reduced time spent resolving scams ($ million) | 46.9 |
| Avoided nuisance cost ($ million) | 10.3 |
| Avoided costs of resolving impersonation scams ($ million) | 49.7 |
| **Total benefit** ($ million) | **196.1** |

Source: *Deloitte Access Economics (2024).* Note: figures may not sum due to rounding

## Total net benefit: voluntary registration

The CBA showed voluntary registration has higher benefits than costs, and a BCR of 1.22. (BCR is a ratio used in a CBA to summarise the overall relationship between the relative costs and benefits of a proposed initiative.

If an initiative has a BCR greater than 1.0, the initiative is expected to deliver a net benefit.) The net benefit (over ten years, in real, present value terms) for voluntary registration is $35.2 million. This is set out in the table below.

**Table 14: Net Present Value (NPV) over 10 years ($ million) for voluntary registration.**

| Costs ($ million) | |
|---|---|
| Government | 20.5 |
| Sender ID users | 126.6 |
| Industry | 13.8 |
| **Total Costs** | 160.8 |
| **Benefits** | |
| Avoided financial cost on scams (consumers) | 89.1 |
| Reduced time spent resolving scams (consumers) | 46.9 |
| Avoided nuisance cost (consumers) | 10.3 |
| Avoided costs of resolving impersonation scams (businesses/entities) | 49.7 |
| **Total benefits** | **196.1** |
| **Net benefit** | **35.2** |
| **BCR** | **1.22** |

Source: *Deloitte Access Economics analysis (2024)*

# Option 3: Mandatory registration of SMS sender IDs

## Costs

This section outlines the costs faced by stakeholders under a mandatory registration scheme. As with Option 2 (voluntary registration) costs are incurred in the financial years indicated or when the Register establishment activities are anticipated by the ACMA to occur.

Specifically, technical costs related to telecommunications industry participants integrating with the Register and sender ID user costs are assumed to commence from the start of 2026 (financial year 2025-26).

### Government

As with option 2, Government costs are sourced from the 2023-24 Commonwealth Budget. The funding has already been appropriated to the ACMA and is considered to not materially differ between policy options. This reflects that the expected technical design of the Register would be comparable across both options. However, unlike a voluntary registration scheme where there is an expectation that government would administer a block list of sender IDs closely related to those already registered, this would not be required for a mandatory registration scheme.

### Telecommunications industry participants

As described in option 2 (voluntary registration) telecommunications industry participants are expected to incur an initial cost upon the creation of the Register and smaller ongoing costs to maintain their systems' integration with the Register. These costs are incurred by the MNOs as well SMS aggregators who may participate in the Register. The assumptions used, and indicative estimates of the feasible incremental costs to MNOs for mandatory registration do not differ from voluntary registration in the CBA and have been estimated using costs from an equivalent Register in Ireland – refer **Table 6**. (Telcos would also likely incur

costs associated with compliance and enforcement activities associated with new Register rules to be developed by the ACMA).

## Sender ID users

As with voluntary registration (Option 2), CBA calculated costs to sender ID users captures both the compliance/administrative costs considered in the CBA as well as registration and fees. While a decision on cost recovery arrangements has yet to be made, it is understood that brands and entities participating in the Register will be charged fees to recover government costs from operating the Register.

In line with this understanding, the fee burden on sender ID users is estimated to be equivalent to the government costs included in the CBA as with voluntary registration.

As with Option 2, costs have been separately calculated for the three user segments, with the high-volume users assumed to incur a system change cost to integrate new business processes and/or technical requirements (refer **Table 7**).

Anticipated user registration rates: mandatory registration

To capture potential registration rates under a mandatory model, intentions have been estimated by DAE through the organisation survey by asking respondents whether they would register under each policy option. The results found **78%** of current sender ID users indicating they would register under a mandatory registration model.

## Sensitivity analysis

The number of sender ID registrations is the primary driver of costs, while the future volume and average loss associated with sender ID scams drive benefits. To illustrate the potential impact of these inputs, DAE conducted a sensitivity analysis to assess the impacts of higher and lower volumes of business registrations, average scam losses and growth in SMS scam volumes. Further detail on the sensitivity analysis may be found in DAE's report.

The results of this sensitivity analysis show that the number of low volume sender ID users has a significant bearing on the results of the CBA. A higher BCR was generated under the high registration sensitivity (1.85 compared to 1.41 under the low registration sensitivity).

Higher and lower bounds of average scam losses were used to further test the sensitivity of results, with the sensitivity range based on historical highs and lows of average SMS scam losses. The analysis shows that the BCR of the mandatory registration option remains above one in both sensitivities (1.93 and 1.22). A modest decrease in scams annually has a material impact on the results with a 5% annual decline resulting in BCRs just above one for the mandatory registration option.

## Total cost to sender ID users

Based on anticipated user registration rates, the total estimated cost (in terms of system change costs and administrative costs to register) for mandatory registration is outlined below. Noting the cost recovery mechanism is to be developed, of note is that the small per user administrative cost of registration and renewal (likely ongoing annual registration costs) spread across many users is the key driver of cost. Registration rates that significantly differ would materially impact the overall cost of registration.

**Table 15: Sender ID user costs: Mandatory registration.**

| Type of cost | Cost ($ million) |
|---|---|
| System change costs | 2.0 |
| Administrative cost, initial | 29.3 |
| Administrative cost, renewal | 17.6 |

Source: *Deloitte Access Economics (2024)*

### Consumers

Consumers are not expected to face any direct costs under this option. As with option 2 (voluntary registration) the CBA noted that while it is possible consumers could experience indirect costs because of telecommunication providers passing on compliance costs, these costs could also be passed on through the A2P SMS supply chain or to sender ID users.

### Regulatory burden estimate

As with Option 2, the estimate of costs to sender ID users captures both the compliance costs considered in the CBA and registration and fees.

**Table 16: Average annual regulatory costs (from businesses as usual), undiscounted over 10 years.**

| Changes in costs ($ million) | Industry | Sender ID users | Consumers | Total change in cost |
|---|---|---|---|---|
| Mandatory registration | 1.7 | 19.8 | - | 21.5 |

Source: *Deloitte Access Economics (2024)*

## Benefits

### Consumers and Sender ID users

The benefits modelled in the CBA represent financial and non-financial benefits that accrue to consumers and sender ID users.

Monetised harms were calculated by DAE for:

- consumers (i.e. financial cost of sender ID scams, time costs of sender ID scams, and nuisance cost of receiving sender ID scams); and
- sender IDs users (i.e. time spent resolving customer complaints) in relation to sender ID impersonation scams

The harms related to sender ID scams are disproportionately associated with the trusted brands that are currently experiencing impersonation. As such, the share of total current harms anticipated to flow from each option is directly related to the share of large sender ID users expected to register due to scammers being unable to spoof registered sender IDs.

The effectiveness of the options in reducing scams in aggregate is also dependent on the response of scammers. For example, Singapore's scam data reveals that while total SMS scams initially decreased 70% during the 3 months immediately after the introduction of a mandatory registration Register, by year's end the total decrease in SMS scams only fell 39% compared to the prior year. To reflect the dynamic nature of scammers adjusting their contact method approach to defraud Australians, the CBA incorporates a five-percentage point annual decrease in the effectiveness of both options (refer Table 17 below).

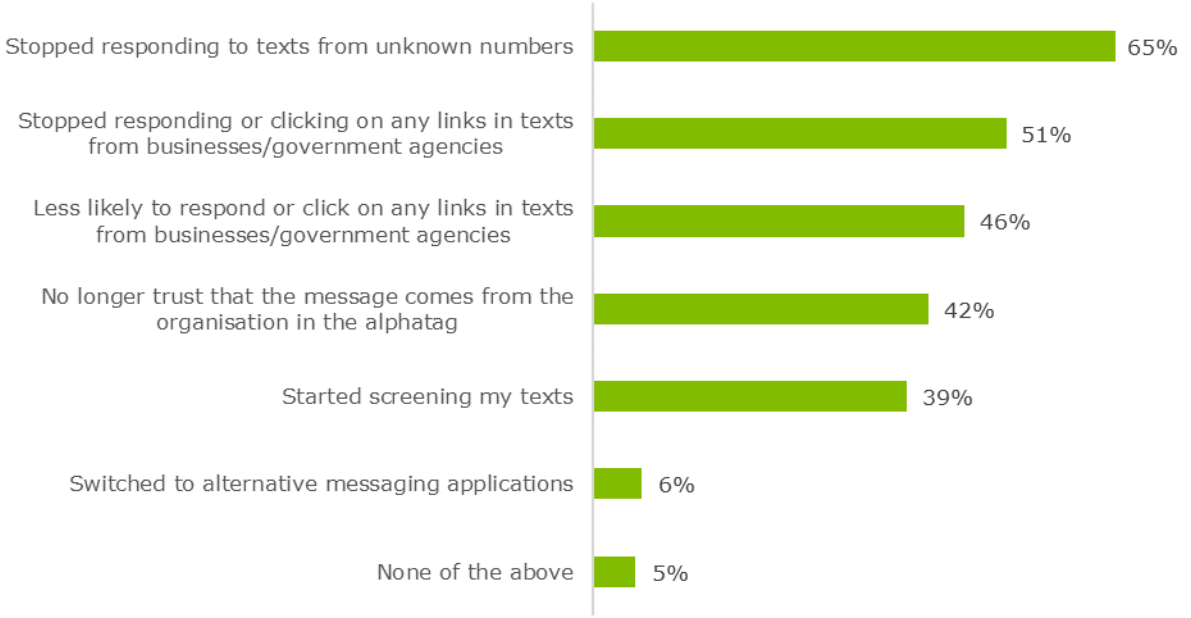
## Trust in SMS as a communications platform

It is envisaged that restoring confidence in SMS as a communications platform – and the financial benefits that flow from this – would be far more likely under a mandatory registration model as it would require SMS traffic with alphanumeric sender IDs to be registered and verified.

The CBA conducted by DAE examined how SMS impersonation scams risk the utility of SMS as a communication platform. This benefit was not quantified but was subject to a qualitative analysis by DAE.

DAE's consumer survey found that 95% of consumers receiving SMS scams have altered how they interact with SMS. This includes not responding to messages, not engaging with messages and no longer trusting that messages from that sender ID are from the legitimate organisation. Additionally, SMS as a platform is negatively affected with 84% of consumers agreeing that scam SMSs have reduced their level of trust in SMS messages as a way of communicating with others. (This is consistent with March 2024 research conducted by *Atomic.io* discussed in Chapter 1, which rated consumer trust and confidence in SMS as a communications channel.)

**Figure 11: Share of consumers reporting changing behaviour in response to SMS scams**




Source: *Deloitte Access Economics (2024)*

The CBA found a reduction in trust negatively impacts organisations using SMS to engage consumers, with 24% of organisations using SMS to communicate with consumers reporting disengagement due to the incidence of SMS scams. The impact is greater for organisations using sender IDs with 35% reporting disengagement.

The top types of disengagement faced by these organisations include:

- contacting customers via SMS to market or sell products (60%);
- receiving payments from customers (53%);
- receiving customers' personal information (51%);
- arranging appointments with customers (43%); and
- customers attending appointments/bookings (43%).

DAE reported almost all (95%) organisations reporting consumer disengagement with SMS also report a corresponding negative impact on commercial outcomes. This includes 72% of organisations reporting an

increase in direct costs such as spending more time and money attempting to contact customers and 40% reporting an increase in indirect costs such as missed appointments or sales opportunities. The size of reported impacts was significant with organisations reporting average direct costs of around $13,000 and an average indirect cost of 7% of affected revenue.

Responses to the organisation survey were not sufficiently representative of the population of sender ID users to extrapolate economy wide costs from these estimates. However, DAE noted if the annual revenue of the respondents to the organisation survey are considered reflective of the top 20% of sender ID users, revenue affected by reduced trust in SMS as a communication platform for businesses amounts to **$7.8 billion annually**.[57] This benefit has not been included in the BCR due to a high degree of uncertainty in the extent of harm reduction that may be realised under each registration option. Additionally, it is unlikely that every dollar of harm reflects forgone revenue, with other impacts including late payments and issues receiving customer information.

## Total benefits: mandatory registration

Total benefits for mandatory registration calculated for the CBA are reflected in the table below.

**Table 17: Total benefits, NPV over 10 years at a 7% discount rate - Mandatory registration.**

| Harm | Mandatory registration |
|---|---|
| Effectiveness rate | 78% |
| Annual benefit decrease | 5 p.p. |
| Avoided financial cost on scams ($ million) | 117.1 |
| Reduced time spent resolving scams ($ million) | 61.7 |
| Avoided nuisance cost ($ million) | 13.5 |
| Avoided costs of resolving impersonation scams ($ million) | 65.4 |
| **Total benefit** ($ million) | **257.7** |

Source: *Deloitte Access Economics (2024).* Note: figures may not sum due to rounding

### Total net benefit: mandatory registration

The CBA showed mandatory registration generates higher benefits than costs and has a BCR of 1.60.

The net benefit (over ten years, in real, present value terms) for mandatory registration is $96.2 million. This is set out below.

---

[57] Based on the reported revenue of organisation survey respondents reporting indirect costs from SMS impersonation scams, average affected revenue amounts to $346,000 for a sender ID user. Applying this value to the 22,500 high and medium volume sender ID users results in the $7.8 billion of estimated impacted revenue.

**Table 18: CBA calculation for mandatory registration, NPV over 10 years at a 7% discount rate.**

| **Costs ($ million)** | |
|---|---|
| Government | 20.5 |
| Sender ID users | 127.3 |
| Industry | 13.8 |
| **Total costs** | **161.5** |
| **Benefits ($ million)** | |
| Avoided financial cost on scams (consumers) | 117.1 |
| Reduced time spent resolving scams (consumers) | 61.7 |
| Avoided nuisance cost (consumers) | 13.5 |
| Avoided costs of resolving impersonation scams (businesses) | 65.4 |
| **Total Benefits** | **257.7** |
| **Net benefits ($ million)** | **96.2** |
| **BCR** | **1.60** |

Source: *Deloitte Access Economics (2024).* Note: figures may not sum due to rounding

# 5. Who did you consult and how did you incorporate their feedback?

The development of the Register's legislative framework has been informed by two tranches of stakeholder and public consultation in 2023 and 2024 to support its establishment and design. These processes have also informed the recommended option for the Register's end state as detailed in this Impact Analysis.

In addition, Deloitte Access Economics (DAE) engaged with specific stakeholders during July and August 2024 as part of its preparation of a cost-benefit analysis (CBA). This work included surveys with businesses and individuals.

Consultation was an important part of the process to assess the expected level of support for the Register and how it would be viewed by stakeholders. Consulting on the type of Register that should be implemented; that is, whether registration of sender IDs should be ultimately voluntary or mandatory, required a specific consultative process. This was to explain and gather information about the expected impact of the two options for sender ID users (current and future across a wide range of sectors) as well as the views of the telecommunications industry and consumer advocacy groups.

The Register will operate Australia-wide across multiple areas of the economy. Accordingly, the department has sought to ensure consultations conducted have garnered views from diverse stakeholders. These include:

- telecommunications providers (including SMS aggregators)
- large businesses and brands
- medium businesses
- small business entities
- banks and financial institutions
- not for profit organisations
- government stakeholders
- consumer organisations
- individual consumers.

## Targeted consultation: February 2023

Targeted consultation was undertaken by the ACMA between 24 February and 17 March 2023 with key stakeholders, including telecommunications providers, government agencies, merchants and consumer organisations. The purpose of the consultation was to gauge the level of support for an SMS Sender ID Register.

The ACMA sent a questionnaire about a potential SMS sender ID register to approximately 70 key stakeholders in February 2023, including telecommunications providers, Government, merchants and consumer organisations. The questionnaire sought views from stakeholders about a number of issues, including:

- whether Australia should implement a Sender ID Register
- the type of Register it should adopt
- who should develop and run the Register
- how it should be funded
- whether it should be enforceable; and
- the benefits and impacts of a Register.

## Summary: outcomes of consultation

Forty-one submissions were received, nearly all of which supported the introduction of a Register in Australia, with more support for a mandatory registration model. Strong support for the introduction of a Register was evident, but responses were mixed regarding the administration of and ultimate nature of the Register. Over half the submissions were in favour of mandatory registration. Overall:

- 21 stakeholders favoured a mandatory registration model
- 10 supported a voluntary registration model, and
- 10 did not indicate a preference or proposed alternative models.

The large majority of submitters (27) preferred a staged or interim implementation approach. Accordingly, the Register has been introduced in stages, beginning with the launch of the Register pilot in December 2023.

Following a decision regarding the nature of the Register and the subsequent development of rules and processes by the ACMA and education strategies, it is envisaged that the staged commencement of Register operations will allow some time for entities to place their user IDs on the Register portal.

# Public consultation: February-March 2024

In February 2024 the Department issued a public consultation paper.

The consultation paper set out the background to the Register, the problem of SMS sender ID impersonation scams, the key features of voluntary registration and mandatory registration and the key benefits and risks associated with each option.

Respondents were asked to provide a written submission or complete a short survey. The consultation sought to gauge:

- if organisations/entities had been targeted by SMS impersonation scams using their alphanumeric sender IDs
- the level of support for a voluntary or mandatory SMS Sender ID Register for alphanumeric sender IDs, and the reasons why; and
- whether any transition arrangements are required to implement the Register.

Survey respondents were asked the following questions:

## Businesses/organisations

- Name, category of organisation/business, and size
- Whether and for what purpose the business/organisation sends SMS with alphanumeric sender IDs
- Whether scammers have used SMS to impersonate the business /organisation in the last 12 months (and how many times); what impact this had; and the likelihood of being targeted in the future
- Whether the business organisation reported the scam and to whom
- Whether registration should be required for all senders of SMS with alphanumeric sender IDs, and reasons
- Whether the business or organisation would pay to register and send SMS with alphanumeric sender IDs
- What alternative methods would be used to communicate if registration was mandatory and the entity was unable or unwilling to pay to Register an alphanumeric sender ID; and
- Other comments

## Individuals

- Whether registration should be required for all senders of SMS with alphanumeric sender IDs, and reasons
- Whether the business or organisation would pay to register and send SMS with alphanumeric sender IDs
- What alternative methods would be used to communicate if registration was mandatory and the entity was unable or unwilling to pay to register an alphanumeric sender ID; and
- Other comments

## Who contributed their views to the consultation?

The departmental public consultation resulted in a total of 111 responses.

- 33 of the responses were written submissions, noting two of the written submissions were from individuals and the remainder from organisations; and
- 78 responses were to the surveys. The survey responses were a combination of individuals and organisations.

With the exception of those submissions marked confidential, written submissions were published on the Department's website.

## Summary of key feedback from the public consultation

Overall **78.1%** of the total respondents from across the written responses and the survey supported the adoption of mandatory registration for sender IDs.

### A. Survey responses

The survey produced 78 responses:

- individual responses made up the majority (75.6%) against organisations/entities (24.4%).
- in total 89.7% of survey respondents supported mandatory registration.

Individuals surveyed

The overwhelming majority of individual respondents surveyed (88%) indicated they had been targeted by an SMS impersonation scam in the last 12 months.

For those individuals who had been targeted, 82.7% reported that this had occurred over 5 times in 12 months. The most notable impacts for individuals were: *"a greater distrust of people you don't know when they contact you"* and *"a greater distrust of websites or apps, banks or telecommunications services".*

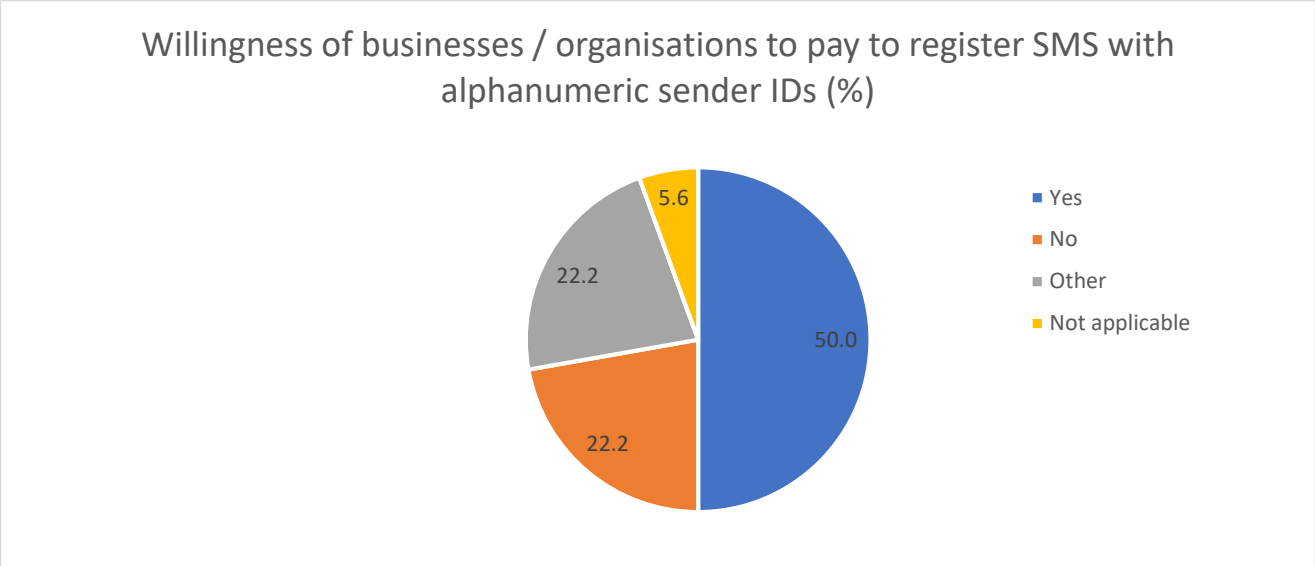
Organisations/entities surveyed

There were 19 organisations/entities that responded via the survey; of these organisations, 17 of 19 (89.4%) supported the mandatory model for the future Register; only one respondent was against the adoption of mandatory registration for sender IDs, with the remaining respondent unsure.

The types of organisations that supported mandatory registration of sender IDs in the survey included banks, financial institutions and not for profit entities.

Organisations and entities targeted by SMS impersonation scams cited reputational damage, financial loss and customer complaints as the main impacts. Despite the limited sample size of 19, the survey revealed the willingness of businesses and organisations to pay in order to register sender IDs varied. Concerns raised were based on additional costs and time to business.

**Figure 12: Willingness of businesses/organisations to pay to register SMS with alphanumeric sender IDs**




Note: 1 null response has been excluded; the table above reflects 18 responses provided. 'Other' responses noted concerns around the costs, including that any charge for using an SMS Sender ID should be based on use / amount of messages sent. Another respondent indicated consideration would be given once the cost is known.

Source: *Department of Infrastructure, Transport, Regional Development, Communications and the Arts; consultation conducted February 2024*

### B. Written submissions

Thirty-three written submission were received by the department.

Overall**, 66.6%** (22 responses) supported mandatory registration – noting one submission noted its support was 'in principle'; **18%** (6 responses) preferred a voluntary solution; 3 respondents (**9%)** submitted it was too early to determine, and 2 respondents did not give a preference.

Five respondents who conveyed support for mandatory registration indicated their desire for additional information regarding the costs, implementation, and design of the Register. Written submissions supporting a mandatory registration model were received from: consumer representative bodies, banks and financial institutions, regulators and peak bodies in addition to larger mobile network operators.

The large majority of submissions noted the importance of an extensive education and awareness campaign prior to the Register's 'end state' launch, and recognised that a transitional period would be required for implementation of the Register.

Views from SMS aggregators were mixed regarding the nature of the end-state Register. Mandatory registration was viewed by a couple of participants as creating implementation and operational inefficiencies and cost barriers. However, other aggregators argued a mandatory scheme would be the best approach, enabling critical brand protection and reducing phishing scams. Comments were made concerning potential cost impacts of mandatory registration, particularly on smaller entities.

Responses that were unsure or supportive in principle included concerns that not enough information had been provided in relation to how the scheme would operate and what additional costs could be expected. In particular these submitters sought more detailed information regarding the implementation process, and raised concerns about increased costs, time commitments and added layers of bureaucracy.

## Key themes emanating from consultation

The responses fell within the four key themes of security, trust, cost and implementation; these are detailed in the table below.

**Table 19: Key themes from 2024 consultation by the Department.**

| Theme | Mandatory Benefits | Mandatory Concerns | Voluntary Benefits | Voluntary Concerns |
|---|---|---|---|---|
| **Security** | Enhanced security by users of SMS sender id registering.<br>Provides a greater level of protection to government, organisations and consumers.<br>Reduces the ability of scammers to create multiple accounts due to verification requirements.<br>Business will have increased protection of their brand and reputation.<br>The need to combat the increasing sophistication of SMS scams. | Requires anyone who wants to use alphanumeric sender IDs to register, irrespective of whether or not they are at risk of being impersonated or regular users.<br>Impersonation scams may continue (in the body of the SMS). | It will benefit brands who want to use it, or are at higher risk of SMS ID impersonation, without impacting other users of alphanumeric sender IDs that are unlikely to be the target of scammers. | Could give consumers false confidence in SMS sent with a sender ID.<br>Scammers more likely to find way to circumvent. |
| **Trust** | Consumers will have an increased sense of trust and less fear of personal loss.<br>Consistency and clarity in determining the authenticity of senders<br>Consumers more likely to engage with businesses using sender ID<br>Ensuring legitimacy of messages creates a 'safe' communications channel. | | | Could give consumers false confidence in SMS sent with a sender ID; they will not be able to readily determine if the sender ID is registered and therefore legitimate.<br>Consumers unable to identify SMS scam impersonation messages will see trust eroded. |
| **Costs** | Although supportive of a mandatory register a number of organisations raised concerns about cost uncertainties. | Unnecessary cost placing an increased burden and an additional layer of bureaucracy on business. | | Participant take up might be lower and this may increase the costs for those who do register. |
| **Implementation** | A number of respondents supportive of a mandatory system requested additional information regarding the implementation process. | Complexities of implementing the new system. | Implementation impacts only the organisations who choose to Register. | Implementation concerns. |

Source: *Department of Infrastructure, Transport, Regional Development, Communications and the Arts; consultation conducted February 2024*

# Consultations conducted as part of cost-benefit analysis: July-August 2024

## Targeted consultation

Further targeted consultation was undertaken by DAE during July and August 2024.

A range of government and business stakeholders were consulted to help inform the CBA and development of DAE's analysis. Stakeholders from the telecommunications industry, participants of the pilot Register (high volume sender ID users), other businesses and overseas regulators with comparable initiatives were consulted through an interview process.

The consulted stakeholders represented the views of consumers and different segments within industry, including small and micro businesses.

## Business and consumer surveys and focus groups

To support the collection of data and define appropriate inputs to inform the CBA model and analysis, primary data collection activities were undertaken in the form of surveys. DAE engaged the market research firm, Dynata, to support in the recruitment of focus groups (for both impacted businesses and consumers) and in the development and distribution of online surveys.

The total response to the surveys were:

- consumer survey: 1,011 responses
- organisation survey: 618 responses (of which, 151 organisations were Sender ID users)

A range of organisations were surveyed, with annual revenues ranging from under $50,000 to over $10,000,000, and number of employees ranging from:

- 0 to 4 (17%)
- 5 to 19 (18%)
- 20 to 199 (28%)
- Over 200 (35%)

Respondents on the surveys were recruited by Dynata through their established market research channels. Eligibility for the consumer surveys was based on location (Australia only) and age (18 years or older). Eligibility for the organisation survey was targeted at sales and marketing professionals in consumer facing Australian businesses.

### Headline results

The organisation survey included a question as to whether there was a preference for voluntary or mandatory registration of sender IDs. As demonstrated in the table below, 68% of current sender ID users favoured mandatory registration:

**Table 20: Organisation survey respondents (that use sender IDs), response to question: In your view, should registration by sender ID users be mandatory or voluntary?**

| Response | Number of organisations | Percentage of organisations |
|---|---|---|
| **Mandatory** | 102 | 68% |
| **Voluntary** | 46 | 30% |
| **Total** | **148** | **98%** |

Source: *Deloitte Access Economics, organisation survey 2024*

# Further opportunities for consultation

Throughout the design and development phases of the Register, there has been, and will continue to be, extensive engagement with relevant stakeholders to identify potential issues and consequences of the Register framework.

The enabling legislation confers new powers on the ACMA to make determinations, by legislative instrument. These instruments will set out further requirements for access to the Register and applications for the registration of sender IDs; and its administration and operation. When developing these instruments, the ACMA will consult extensively with affected stakeholders; in particular, the telecommunications industry (mobile network operators and SMS aggregators).

The use of legislative instruments to specify these requirements will be critical in allowing functional aspects of the Register's operation to be adjusted over time to accommodate both changes in technology and services that may be part of the Register in the future. It will also provide agility to respond to changes in scammers' behaviour, while providing ongoing increased protection to legitimate entities and consumers.

# Conclusions

Results of the consultation processes, along with feedback received in submissions, have been considered in shaping the approach to progress the future Register.

Notably, all three consultation processes conducted indicate that significantly more stakeholders favour mandatory registration for sender IDs over voluntary registration for the 'end state' Register.

Consultations with affected stakeholders will continue as the Register's design progresses. The ACMA will engage with industry and other key stakeholders during 2025 to develop legislative instruments relating to the Register's administration and operation.

# 6. What is the best option from those you have considered and how will it be implemented?

## What is the best option? The Decision Rule

The decision rule used to assess the three options outlined in Question 3 was to select the option that delivers the greatest net benefit to consumers and businesses and would best meet the Government's objectives.

Of the three presented options, Option 3 presents the greatest net benefit and most effectively delivers on the regulatory objectives associated with preventing SMS sender ID impersonation scams. This option effectively addresses the Government's commitment to safeguard consumers and entities against SMS sender ID impersonation scams by protecting the legitimacy of SMS sender IDs.

Consideration of each option is outlined below. It should be noted that the following assumptions apply across all three options:

- individual telcos will continue to develop and trial new anti-scam measures to disrupt SMS scams, and
- new arrangements under the Scams Prevention Framework in a *revised Competition and Consumer Act 2010* – including a new code for the telecommunications industry – is anticipated to be in place in 2026 and is expected to further bolster anti-scam measures for SMS.

### Option 1 – Maintain the status quo (no change)

Option 1, the status quo, fails to address the present problem concerning SMS sender ID impersonation scams and does not deliver any identified policy objectives of the Register framework.

Under this option, it is anticipated SMS messages with sender IDs would continue to be subject to sender ID impersonation by scammers – causing ongoing harm to consumers and to the reputation of retail brands and government entities. Option 1 does not address the Objectives of Government Action (see Chapter2), nor does it align with stakeholder and community support of the implementation of an SMS Sender ID Register, as evidenced in consultation processes conducted in 2023 and 2024.

### Option 2 – voluntary registration of sender IDs

This option meets the Register objectives to a limited extent.

Voluntary registration would offer increased protections for entities, but this would be for registered users only. It is anticipated that under voluntary registration, scammers would turn their focus to target those businesses and entities not registered, or would attempt to use variations of registered sender IDs that have not yet been placed on a blocklist.

As a consequence, members of the public would likely continue to receive scam SMS impersonating brands that have not registered. Consumers would not readily know which brands and entities are protected via registration and which entities are not, leaving them vulnerable to scams and/or distrustful of all SMS with alphanumeric sender IDs.

### Option 3 – mandatory registration of sender IDs

This option effectively addresses limitations in the current regulatory framework to ensure consistent outcomes for alphanumeric sender IDs.

It provides a very high level of protection to consumers, as SMS traffic with alphanumeric sender IDs will only reach consumers where the sender ID is registered and originates from a legitimate sender. SMS with unregistered alphanumeric sender IDs will be blocked or tagged as possible scams.

All brands/entities using sender IDs would be protected.

This option received widespread support (over 70%) as the preferred implementation option for the Register in consultation conducted to date by both the department and DAE as part of the CBA.

## Preferred option

Option 3 (the mandatory scheme) is considered the most effective of the options to meet the objectives of an SMS Sender ID Register.

Option 3 carries the highest net benefit for consumers and entities as detailed in Chapter 4. While the costs of Option 2 and Option 3 are similar, the benefits are highest under the mandatory registration option. Under the mandatory option, consumers receive **$192 million** in benefits from avoided financial costs and avoided time spent resolving scams, while sender ID users received **$65 million** in benefits.

The CBA indicates that Option 3 has a BCR of 1.60 with the benefits of avoided costs of scams outweighing the costs to industry and government.[58] The voluntary scheme (Option 2) also has higher benefits than costs, but a relatively lower BCR of 1.22. The net benefit (over ten years, in real, present value terms) is **$96.2 million** under Option 3 and **$35.2 million** under Option 2.

**Table 21: Primary results of the CBA, comparing voluntary and mandatory registration, net present value (NPV) over 10 years ($ millions).**

| | Option 3-Mandatory registration | Option 2-Voluntary registration |
|---|---|---|
| **Costs** | | |
| Government | 20.5 | 20.5 |
| Sender ID users | 127.3 | 126.6 |
| Industry | 13.8 | 13.8 |
| **Total costs** | **161.5** | **160.8** |
| **Benefits** | | |
| Avoided financial cost on scams (consumers) | 117.1 | 89.1 |
| Reduced time spent resolving scams (consumers) | 61.7 | 46.9 |
| Avoided nuisance cost (consumers) | 13.5 | 10.3 |
| Avoided costs of resolving impersonation scams (businesses) | 65.4 | 49.7 |
| **Total benefits** | **257.7** | **196.1** |

---

[58] BCR is a ratio used in a CBA to summarise the overall relationship between the relative costs and benefits of a proposed initiative. If an initiative has a BCR greater than 1.0, the initiative is expected to deliver a net benefit.

| | Option 3-Mandatory registration | Option 2-Voluntary registration |
|---|---|---|
| Net benefit | 96.2 | 35.2 |
| BCR | 1.60 | 1.22 |

Source: *Deloitte Access Economics (2024).*

The table on the following page denotes whether Register objectives are expected to be met, somewhat met, or not expected to be met against both options.

**Table 22: Comparison: Mandatory registration and voluntary registration against register objectives.**

| Objective | MANDATORY registration | VOLUNTARY registration |
|---|---|---|
| Decrease the frequency and impact of SMS impersonation scams on consumers (where impersonation occurs in the sender ID) | Expected – provides a very high level of protection to consumers, as SMS traffic with alphanumeric sender IDs will only reach consumers where the sender ID is Registered and originates from a legitimate sender. All other SMS with alphanumeric sender IDs will be blocked or tagged e.g. 'Likely scam')[59] CBA analysis indicates $192M in consumer benefits from avoided costs and time spent resolving scams. | Somewhat expected – noting voluntary registration would not stop criminals targeting businesses and entities who have not registered alphanumeric sender IDs. Consequently, members of the public would likely continue to receive scam SMS impersonating brands that have not registered. CBA analysis indicates $146M in consumer benefits from avoided costs and time spent resolving scams under voluntary registration. |
| Increase protections for legitimate brands and agencies against bad actors impersonating them | Expected – all brands/entities using sender IDs (that are Registered under a mandatory registration model) would be protected; scammers would not be able to target businesses and entities via use of alphanumeric sender IDs that have not been registered, as this SMS traffic would be tagged as possible scam or blocked. | Expected – but increased protections would be for registered users only. All other sender IDs utilising alphanumeric sender IDs that are not registered would not be protected. |
| Disrupt the business models for SMS impersonation scams | Expected– impersonation via SMS sender IDs would be significantly disrupted as a scam mechanism as scammers would not be able to sequentially target entities via use of alphanumeric sender IDs that have not been registered. | Somewhat expected – but it is anticipated that under voluntary registration, scammers would turn their focus to target those businesses and entities not registered. |
| Restore public confidence in SMS as a communications channel | Expected– all unregistered SMS with alphanumeric sender IDs will be blocked or tagged as fraudulent, giving consumers confidence that SMS which appear in existing message streams are legitimate. | Improbable / not expected – consumers would not readily know which brands and entities are protected via registration and which brands and entities are not, leaving them vulnerable to scams and/or distrustful of all SMS with alphanumeric sender IDs. |
| Ultimately, make Australia a harder target for scam activity | Expected – the presence and enforcement of a Register will strengthen overall protections against scam activity. | Expected – the presence and enforcement of a Register will strengthen overall protections against scam activity. |

Source*: Department of Infrastructure, Transport, Regional Development, Communications and the Arts; consultation conducted February 2024*

---

[59] Operational details pertaining to the Register are yet to be finalised, including whether non-compliant SMS with alphanumeric sender IDs will be blocked or tagged as fraudulent.

# Implementation

It is proposed that implementation of Option 3 would be given effect through an industry standard made by the ACMA under existing powers in the *Telecommunications Act 1997*. The standard would bind telecommunications providers (including SMS aggregators) involved in SMS traffic to certain obligations; i.e. SMS traffic with alphanumeric sender IDs would not be able to be sent, or sent with warnings/tags unless it complied with rules set out in the standard.

The new *Telecommunications (SMS Sender ID Register) Act 2024* establishes the key elements of the Register framework. The use of secondary legislation, such as determinations to be made by the ACMA, enable the framework to be adjusted and amended over time to reflect changes in technology and behaviours adopted by scammers.

Implementing any new framework carries a number of intrinsic risks, including whether the framework is effective in meeting its intended objectives, whether it places unintended burdens on stakeholders and in its ability to adjust to technological advancements. Throughout the design and development phases of the Register, there has, and will continue to be, extensive engagement with relevant stakeholders to identify potential issues and consequences of the Register framework.

It is recognised that a mandatory registration framework recommended under Option 3 would impose costs on current and future SMS sender ID users, and be an additional regulatory impost for telecommunications service providers. In addition, data captured through surveys and stakeholder consultations conducted by DAE indicates some industry participants hold concerns regarding the additional regulatory cost to users to become registered, specifically for smaller businesses, as well as the capacity of telecommunications providers to effectively implement the Register.

## Measures to support implementation

To support successful implementation of Option 3, the following strategies and measures are proposed.

### A period of transition to implement mandatory registration of sender IDs

The enabling legislation allows for delayed commencement of the Register. A period of transition is expected in recognition that the Register will need to deploy a complex ICT mechanism capable of interacting with systems and processes used by the telecommunications industry with robust privacy and security settings. It is also recognised the ACMA will require additional time to finalise preparations for the Register and prepare related instruments. The ACMA has flexibility about when the Register becomes operational; it is anticipated the Register could be expected to be operational by late 2025. However, as noted in the Explanatory Memorandum to the legislation, the Register's commencement 'may involve entities submitting and registering their sender identifications during a transition period, prior to the Register being fully operational'.

### Effective engagement with the telecommunications industry

It is intended the ACMA would engage with Communications Alliance to ensure relevant providers are aware of and understand the introduction of new enforceable obligations. This may include providing additional guidance leading up to and following the introduction of the standard. As part of the development of the industry standard, consultation will occur with telecommunications providers and other interested stakeholders to potentially address any implementation concerns that industry may have and encourage ongoing best practice.

### Effective education strategies for current and future sender ID users

Ensuring the registration process is straightforward will be crucial when launching Register operations. The enabling legislation provides for a 2-stage registration process whereby entities first Register with the ACMA and undergo verification checks before submitting sender IDs for registration. The enabling legislation's Explanatory Memorandum notes that submitting this information would likely involve an interactive online

portal, such as ACMA Assist. It is envisaged that the ACMA would publish information and guidance setting out how an applicant would register for approval. (Currently, the ACMA publishes a registration guide for ACMA Assist, which provides step by step instructions on how to register; it is anticipated a similar approach would be taken for the Register.)

As noted, there is no 'silver bullet' to eliminate scam activity. Whilst it is expected that Option 3 will have a significant impact on scam reduction for sender ID impersonation scams and strengthen the ecosystem as a whole against scam activity in Australia, it is also expected that scammers will pivot to other methods to defraud consumers.

# 7. How will you evaluate your chosen option against the success metrics?

## Measurement of success

### Measurable indicators

Measurable success indicators of the new Register framework being implemented against option 3 (mandatory registration) will include:

- a decrease in reported financial losses to Scamwatch for SMS scams (including SMS impersonation scams);
- a decrease in reported SMS sender ID impersonation scams, as reported to Scamwatch (see section below); and
- a decrease in losses from SMS sender ID impersonation scams, as reported to Scamwatch (see section below).

A key indicator of the success of the Register's implementation against option 3 mandatory registration will be a reduction in harm experienced by consumers and as reported to Scamwatch, including harms experienced by First Nations people and CALD communities, both of which are currently over-represented in financial losses to scams.

While it is expected that there will be an overall decrease in SMS sender ID impersonation scams, it is also likely that the launch of the new Register will generate an influx of complaints to the ACMA in the initial stages. This may result from consumer confusion concerning the Register's remit; that is, consumers may not understand the difference between SMS impersonation sender ID scams (where impersonation occurs in the message header) and SMS impersonation scams where the impersonation occurs in the body of the SMS message.

### SMS blocking vs a decrease in the initiation of SMS sender ID impersonation scams

The introduction of the SMS Sender ID Register will complement existing obligations under the Scams code, which requires Australian telecommunications service providers to proactively identify, trace, and block scam SMS. New arrangements under the Scams Prevention Framework in a revised Competition and Consumer Act 2010, including a new code for the telecommunications industry is anticipated to be in place in 2026.

It is yet to be determined whether telecommunications service providers will also be required to block – or tag as fraudulent – those SMS that do not comply with (future) Register rules.[60]

Since July 2022 to 30 June 2024, industry has reported blocking over 668.3 million scam SMS. The enormous volume of blocked scam SMS illustrates the effectiveness of the Code requirements to block SMS. However, it also indicates that very large numbers of scam SMS continue to be initiated.

While SMS blocking numbers may provide a basis by which to assess the industry compliance with the Code (and possibly with the Register), a significant decrease in the initiation of SMS sender ID impersonation scams by bad actors would signal that scammers' business models have been significantly disrupted by the

---

[60] These rules will be developed and made by the ACMA following a Government decision on the type of Register that will be implemented (voluntary or mandatory registration).

implementation of the Register. This is a policy objective of the Register. The preferred option of mandatory registration is expected to generate a sizeable decrease in the volume of these scams being initiated in the first place. In this sense, the implementation of Option 3 is expected to act as a deterrent to prevent this subset of SMS scams by disrupting the business models of bad actors sending fraudulent SMS impersonating entities.

## Other indicators

In addition to directly measurable success indicators, it is expected that Option 3 will significantly restore trust in SMS with alphanumeric sender IDs as a communications channel. DAE's analysis indicated that 95% of consumers who have received an SMS scam have altered how they interact with SMS as a result.[61] It is expected that adopting mandatory registration of sender IDs under the Register will boost consumer confidence in SMS as a communications channel – a key policy objective of the Register – by safeguarding the legitimacy of SMS with alphanumeric sender IDs.

It is further anticipated that Option 3 mandatory registration will decrease in the time and resources spent combating scam activity as reported by businesses and entities.

## Monitoring and evaluation

The implementation of Option 3 mandatory registration for sender IDs would be a new regulatory intervention in Australia.

As such, it will be important for the operation and effectiveness of the new arrangements, once implemented, to be carefully assessed. The review would consider the operation of the framework and the extent to which it has supported the overall objective of protecting Australian consumers and businesses against SMS impersonation scams.

Compliance with the Register framework and industry relating to the Register will be monitored. Changes in SMS sender ID impersonation scam patterns and behaviours will also be monitored.

Should Option 3 be chosen, a monitoring and evaluation program for the reforms will be established. The program will be developed in line with the Commonwealth Evaluation Policy, which provides for a principles-based evaluation approach that is fit-for-purpose, useful, robust, ethical, culturally appropriate, credible, and transparent where appropriate.

The monitoring and evaluation program will include an evaluation framework, program logic and post-implementation review designed to measure a wide range of outcomes relevant to SMS sender ID impersonation scams and their impacts on Australian businesses and consumers. The program will measure reduction in rates of SMS sender ID impersonation scams.

The evaluation framework will be targeted and adaptable to the specific aims and outcomes of the relevant measures contained in Option 3. It will incorporate both existing and to-be-developed datasets, information sources and international comparisons (where available).

## Collection of new datasets by the NASC

The National Anti-Scam Centre (NASC) has developed an additional field in its Scamwatch form to identify SMS impersonation scams where the impersonation occurs in the message header of the SMS. (Previously, the Scamwatch form did not collect 'sender IDs', just numeric phone numbers). The reporting form does

---

[61] *SMS Sender ID Register Cost-Benefit Analysis:* Deloitte Access Economics, September 2024 p.23

include a field for ‘impersonated entities’ for all scam reports which may coincide with sender IDs in some scams.

Changes to the Scamwatch form incorporating this data field went live in September 2024. Early data provided by NASC for the period from the 6th to the 30th September, since the commencement of the new data field, reported 126 scam messages where the impersonation occurred in the sender ID. The scam messages impersonate a broad range of entities including government, and businesses.

Collection of this new data field will significantly assist the Government in measuring the success of the new SMS Sender ID Register and how it meets the original objectives of the Register.

It is anticipated that by the time the Register framework is implemented – which could be late 2025 – this specific data will give a more accurate picture of the number of SMS sender ID impersonation scams.

This will provide Government with insights into SMS sender ID scam impersonation trends, and compliance and enforcement activity under the new framework. In turn, this will enable policy settings to adapt as needed to drive desired outcomes against SMS sender ID impersonation scams.

## Ongoing evolution of the success metrics

Following the implementation of the Register framework, it is anticipated the ACMA, will develop a program to monitor compliance with the new enforceable obligations under the Register framework; this is intended to include receiving, investigating, and monitoring complaints in relation to potential breaches.

Monitoring compliance with new obligations under the Register’s framework and taking enforcement action where necessary will be key to the Register’s operational success. Implementation of a mandatory registration scheme for sender IDs will be given effect through an industry standard made by the ACMA[62] under existing powers in the *Telecommunications Act 1997*. The standard will set out rules for telecommunications providers involved in sending SMS traffic.

This will lead to enquiries, investigations and, where necessary, compliance and enforcement action, taken using ACMA’s powers in the *Telecommunications Act 1997*. The information obtained in investigations will also contribute to evaluating the effectiveness of the Register framework as a whole and will allow for the iterative evolution of the performance metrics.

If a telecommunications provider does not comply with rules set out in an industry standard, they will be subject to enforcement action by the regulator. The ACMA has a number of enforcement options available for breaches of an industry standard from formal warnings to civil penalties of up to $250,000.

If certain facets of the Register framework prove ineffective against its intended outcomes or a weakness is identified, the ACMA may consider varying the Register framework instruments (industry standard and/or subordinate instruments) to ensure that the risk of Australians being exposed to SMS sender ID impersonation scams is effectively managed. Variation may also be necessary given the evolution of technologies used by scammers and the dynamic nature of scammer behaviour.

---

[62] If directed by the Minister under the *Telecommunications Act 1997.*

# Abbreviations and Glossary

| Term | Definition |
|---|---|
| A2P | Application-to-person messaging, where SMS are sent from a business application to mobile users via an automated process. |
| ABS | Australian Bureau of Statistics |
| ACCC | Australian Competition & Consumer Commission |
| ACMA | Australian Communications and Media Authority |
| ACMA Act | means the *Australian Communications and Media Authority Act 2005* |
| AI | Artificial intelligence |
| Alphanumeric sender IDs | The alphanumeric name that appears in the message header of an SMS that identifies who (usually a company name or brand) sent the message. |
| BCR | Benefit-cost ratio. BCR is a ratio used in a CBA to summarise the overall relationship between the relative costs and benefits of a proposed initiative. If an initiative has a BCR greater than 1.0, the initiative is expected to deliver a net benefit |
| CALD | Culturally and linguistically diverse communities |
| CBA | Cost-benefit analysis |
| CSPs | Carriage Service Providers |
| ComReg | Commission for Communications Regulation (Ireland) |
| MMS | Multimedia Messaging Service |
| MNO | Mobile Network Operator; provides a network and services to its subscribers |
| NASC | National Anti-Scam Centre |
| NPV | Net present value.<br>The NPV measures the benefits of pursuing an option (relative to the status quo), minus the costs of pursuing that option (also calculated relative to the status quo), with a discount rate applied to place less weight on future costs and benefits than present costs and benefits. Where the NPV is positive, the benefits of pursuing the option outweigh the costs. |
| Phishing | Phishing occurs when cyber criminals trick consumers into giving them personal information. They do this by sending fraudulent emails or SMS messages often pretending to be from large, known and trusted organisations. They may try to steal online banking logins, credit card details or passwords. Phishing can result in the loss of information, money or identity theft. |
| Scam | A fraudulent scheme performed by a dishonest or deceitful individual, group or company in an attempt to obtain money or something else of value. |
| Scammers | A person who commits fraud or participates in a dishonest scheme. |
| Scamwatch | Website run by the ACCC providing information to help individuals identify and avoid scams |
| SMS | Short Messaging Service |
| SMS Aggregator | SMS aggregators are the gateway between carriers and text messaging software providers. Australian businesses can use a messaging gateway to send bulk text messages for alerts, marketing and communication campaigns or 2-way messages via a gateway network |
| SMS Impersonation Scams | Fraudulent SMS message appearing in the message header of an SMS, pretending to be from a known and trusted organisation. |
| Smishing | Phishing by SMS |
| Spoof | A type of attack where the message is made to look like it comes from a trusted source. |
| Telcos | The term for telecommunications providers |
| WTP | Willingness to pay |

# Appendix A – Cost-Benefit Analysis

See separate attachment to this document.