Deloitte.

SMS Sender ID Register

Cost-Benefit Analysis

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

Final Report – 11 October 2024

Deloitte Access Economics

Contents

Tables

Glossary

Acronym	Full name
A2P	Application-to-person
ABS	Australian Bureau of Statistics
ACCC	Australian Competition and Consumer Commission
ACMA	Australian Communications and Media Authority
ACT	Australian Capital Territory
BCR	Benefit-cost ratio
CBA	Cost-benefit analysis
FY	Financial year
ID	Identification
MNO	Mobile Network Operator
NPV	Net present value
NSW	New South Wales
NT	Northern Territory
OIA	Office of Impact Assessment
OTT	Over-the-top
p.a.	per annum
QLD	Queensland
RCS	Rich Communications Services
SA	South Australia
SMS	Short Message Service
TAS	Tasmania
VIC	Victora
WA	Western Australia
WTP	Willingness to pay

Executive summary

Purpose of this engagement

In April 2023, the Minister for Communications announced the establishment of a SMS Sender ID Register (the Register), which will be established and maintained by the Australian Communications and Media Authority (the ACMA). The Register is designed to protect consumers and brands by disrupting a specific type of SMS scam – alphanumeric sender ID impersonation scams referred to as 'sender ID scams' hereafter – where scammers send SMS with sender IDs to imitate well-known brands such as banks, government agencies or retailers to deceive victims, to steal their money or personal information.

The government is considering whether registration of sender IDs on the Register will be under a voluntary or mandatory registration scheme for users. In February 2024, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts (the Department) conducted public consultation on both options, which included a consultation paper containing an overview of both voluntary and mandatory registration, and a survey.

Deloitte Access Economics has been engaged by the Department to develop a cost-benefit analysis (CBA) of the two registration schemes for establishing the Register. 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 users and consumers from avoided sender ID scams.

The problem of sender ID scams

Scamwatch reports that SMS scams have grown significantly in recent years, now making SMS the most commonly reported method used by scammers to target Australians. Sender ID scams are a particularly insidious form of SMS scam due to their ability to impersonate legitimate organisations more convincingly and to appear in the same message stream as legitimate communications with trusted brands. While it is estimated based on industry consultation that there are approximately 300,000 sender IDs currently in use in Australia, the greatest risk of impersonation is generally accepted to lie with the smaller portion of large, well-known and trusted brands (such as the Australian Taxation Office, MyGov, Australia Post, large banks, and toll operators).

The financial cost of sender ID scams is significant, with estimates produced for this CBA totalling $26.6 million across approximately 108,000 scams in 2023. However, the harms extend beyond the financial costs. Scammed consumers waste time attempting to resolve issues related to being scammed such as recovering access to online accounts and changing passwords, while businesses that are impersonated spend time resolving customer issues related to being scammed.

Sender ID scams also threaten the utility of SMS as a way for Australians to communicate. Consumers regularly receiving sender ID scams face the nuisance of assessing what communication is legitimate. In fact, the consumer survey undertaken for this CBA found that 84% of consumers agree that scam texts have reduced their level of trust in SMS as a way of communicating with others. A loss of trust also contributes to decreased engagement with SMS communication received, with 51% of consumers no longer opening or clicking on links in SMS messages that come from businesses or government.

A loss of trust and engagement could threaten the utility of SMS as a communication channel for business, government and other organisations. There is evidence this is already occurring. The organisation survey undertaken for this CBA found that 35% of sender ID users report experiencing additional difficulty engaging consumers through SMS. These organisations report a corresponding decrease in revenue through missed appointments and difficulty gathering customer information, as well as increased costs of investing in other communication channels.

The Register and its impacts

The Register aims to reduce SMS scams that use sender IDs to impersonate legitimate organisations. Reducing SMS scams aims to minimise the associated financial losses and time costs imposed on consumers and businesses to resolve sender ID scams, as well improving trust in SMS as a communication platform.

Implementing a Register will impose costs on government to establish the Register, manage the registration process of sender IDs and maintain the Register. Telecommunication industry participants also face costs to integrate and comply with the Register, while sender ID users (which includes all types of organisations who use sender IDs such as businesses, government entities and not-for-profits) will incur a range of administrative, system change and direct financial costs associated with registering sender IDs.

It is understood that the Register (regardless of whether registration of sender IDs is voluntary or mandatory) will operate on a 'user pays' basis, as a cost-recovery model. 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. Fees on industry were not quantified as part of the CBA, however, they may in practice influence registration rates.[1] The impact of fees is considered as part of the regulatory burden estimates in this report and potential variability in registration rates has been assessed through testing of higher and lower bounds of registration under each option.

Approach to cost-benefit analysis

This report considers two different registration schemes for the Register and undertakes a CBA of each scheme. Costs and benefits are assessed across government, industry, sender ID users and consumers over a 10-year period, relative to a base case in which the Register is not established (the status quo).

The two Register schemes assessed were:

- **Option 1 – Mandatory Registration.** A mandatory scheme would require organisations to apply to register any sender IDs used to send SMS to Australian mobile phones if they want to continue using those IDs without them being blocked or potentially labelled as 'likely scam' or similar. Telecommunications companies would be subject to enforceable rules (under an industry standard) under this scheme, whereby they would be required to block SMS with sender IDs or label them as 'likely scam' or similar unless they were registered and the sender is verified as the registered party. If an entity did not wish to register their sender IDs, they could use phone numbers as sender IDs instead, to avoid SMS being blocked or labelled as scams, or other forms of communication.
- **Option 2 – Voluntary Registration.** A voluntary registration scheme would allow entities wishing to send messages with sender IDs to choose to apply to register those identifications. Telecommunications companies would be subject to enforceable rules requiring them to check registered sender IDs to determine whether the sender is the registered party, and block or label as 'likely scam' those that don't. Users with unregistered sender IDs would not be impacted by the register.

Deloitte Access Economics undertook a literature review, which informed understanding of the feasible costs and benefits associated with the Register and helped develop data collection methods and tools. These methods included business and consumer surveys and industry consultations. Survey results informed the raw data inputs for the CBA, which were validated based on qualitative insights from the industry consultations and the literature.

The costs and benefits assessed are outlined in Table i, with detailed assumptions presented in Section 3 and Appendix A.

[1] Costs of operating the Register are accounted for in the CBA as a cost to government. Recovery of these costs from brands or entities participating in the Register would mean these would become costs to industry rather than government but would not affect the overall CBA results. The regulatory burden estimates reports total estimated burden both with and without full recovery of cost. Subsequent decisions on the level of cost recovery may influence registration rates under either a mandatory or a voluntary scheme.

Table i: Costs and benefits included in the CBA

Category	Stakeholder	Quantified
Costs		
Register establishment and operation	Government	Yes
Register implementation and compliance	Telecommunication industry	Yes
Registration and administrative costs	Sender ID users	Yes
System changes	Sender ID users	Yes
Benefits		
Reduced financial cost of sender ID scams	Consumers[2]	Yes
Reduced time spent resolving sender ID scams	Consumers	Yes
Reduced nuisance cost of receiving sender ID scams	Consumers	Yes
Reduced time spent resolving impersonation scams	Sender ID users	Yes
Avoided customer engagement costs / enhanced trust in SMS as communication channel	Sender ID users	No

Source: Deloitte Access Economics analysis.

Results

The CBA indicates that the mandatory scheme (Option 1) has a benefit-cost ratio (BCR) of 1.60 with the benefits of avoided costs of scams outweighing the costs to industry and government.[3] 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 1 and $33.3 million under Option 2. Table ii summarises the results.

Table ii: Primary results of the CBA, net present value (NPV) over 10 years ($ millions)

	Option 1 (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

[2] Financial losses from sender ID scams comprise both consumer and business losses.
[3] 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 1 (Mandatory registration)	Option 2 (Voluntary registration)
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**
Net benefit	**96.2**	**35.2**
BCR	**1.60**	**1.22**

Source: Deloitte Access Economics analysis.

The number of sender ID registrations is the primary driver of costs to industry, while the future volume and average loss associated with sender ID scams drive benefits. To illustrate the potential impact of these inputs, sensitivity analysis was conducted to assess the impacts of higher and lower volumes of business registrations, average scam losses and growth in SMS scam volumes.

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. All options remain above a BCR of 1 under the high and low registration sensitives, with the mandatory registration option receiving the higher BCR in both (1.85 and 1.41).

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 sensitives (1.93 and 1.22) but that the voluntary registration option is not (1.47 and 0.93). 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 and below one for the voluntary registration option (1.03 and 0.79 respectively). However, the BCR of the mandatory registration option is higher than the voluntary option under all sensitivities.

Conclusion

The CBA suggests that the Register will generate significant benefits for consumers by reducing the costs associated with SMS sender ID impersonations. The difference between the mandatory and voluntary options explored in this report is not simply about differences in registration rates and, in fact, we find the impact of registration rates on the CBA to be minor. The difference in results between the two options is due to the very operation of the scheme. While the mandatory scheme results in a full list of allowable sender IDs, with any others being blocked or labelled 'likely scam'; the voluntary scheme continues to permit non-registered sender IDs, which may be either legitimate or from scammers, resulting in costs to the economy. So while the costs of either scheme 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 costs of the Register are significant under both options. While government and telecommunication providers face relatively modest costs, business users face approximately $127 million in administrative costs under both registration options due to similar volumes of business registrations. The organisation survey conducted for this CBA found that 75% of businesses would register under the voluntary option, and that 78% of businesses would register under the mandatory option. Business costs are primarily driven by a large volume of smaller businesses that face compliance costs (in terms of time and materials) to register. As such, the analysis indicates that the costs to sender ID users across the whole-of-economy exceed the estimated benefits they receive directly (noting, of course, organisations' interest in benefits accruing to their customers).

The costs will vary depending on the timing of any requirement to register. The CBA assumes that all sender ID users that register do so in late-2025, once the Register is operational. As such, economy-wide upfront costs are highest in that year. After year three, costs estimated in the CBA are primarily driven by the administrative cost of undertaking renewals of sender ID registrations, which is assumed to occur annually – noting that no decision of incurring annual fees has been made and would form part of the formal decision regarding the Register's cost-recovery mechanism. If users were required to renew registration less frequently, costs would also be reduced. Precise costs for telecommunication providers are unknown at this stage due to uncertainties in the technical design of the Register under either scheme. However, the costs are considered by stakeholders to be similar under either scheme.

Survey results suggested variation in sender ID user costs were dependent predominantly on the volume of users rather than the type of user (e.g. by organisation size or type of industry). This indicated that a large number of sender ID users will incur small individual administrative costs to register under either scheme. As the risk of sender ID scams are concentrated among larger, high-profile organisations and trusted brands, the registration of sender IDs associated with small and medium sized entities drives costs but not benefits.

The CBA indicates that the benefits outweigh the costs for both mandatory registration (Option 1) and voluntary registration (Option 2), with mandatory registration delivering a greater net benefit. However, the sensitivity analysis shows that the BCRs are sensitive to changes in the volume and average financial loss associated with SMS scams.

The result of the CBA aligns with the stated preferences of consumers, with 71% of surveyed consumers agreeing that a Register which provides verification that SMS communication was from a legitimate organisation would increase their trust in SMS as a platform. Sender ID users too are in favour of action, with 68% of sender ID users preferring the mandatory registration scheme.

The benefits estimated within the BCR only reflect those that can be monetised and quantified. The impact that increasing trust in SMS as a communications channel may have on sender ID users' costs is included qualitatively. These benefits may be substantial with calculations suggesting the harms are currently as large as $7.8 billion in affected revenue annually such as missed appointments, late payment from customers and forgone revenue due to issues contacting customers. This benefit has not been included in the BCR due to a high degree of uncertainty in the extent of harms reduction that may be realised under each registration scheme.

The data captured through surveys and stakeholder consultations indicate that both consumers and sender ID users support the introduction of the Register – which is expected to lead to continued and, potentially, enhanced use of sender IDs. Some industry participants, however, report concern regarding the additional regulatory cost to users to become registered, specifically for smaller businesses, as well as the capacity of the telecommunications network to effectively implement the Register. The concerns raised emphasise the value in considering a transition period for implementation of the Register and for incorporating effective education and communication strategies, and ensuring the registration process is straightforward.

In preparing this CBA, it is worth recognising the evolution of digital communications channels over time creates uncertainty the further into the future benefits and costs are calculated. Put simply, ten years is a long time in digital communications. If use of SMS was dramatically higher or lower in a decade, this would affect the results. As one more sensitivity test, we present the figures based on a five-year horizon, finding that even in the relative short term both schemes result in net benefits.

Based on these conclusions, this report provides insights into the potential costs and benefits of both registration schemes under consideration for the Register, which can be used to inform government's decision on the preferred approach. The results illustrate both the potential value that can be generated through the introduction of a Register and the need to appropriately consider how any new regulatory requirements are implemented and enforced.

1 Introduction

This chapter outlines the context for this report and the purpose of the cost-benefit analysis, including:

- the current impact of SMS sender ID scams on consumers and businesses
- the intent of the proposed Register
- international examples of similar registers
- the scope of the analysis in this report.

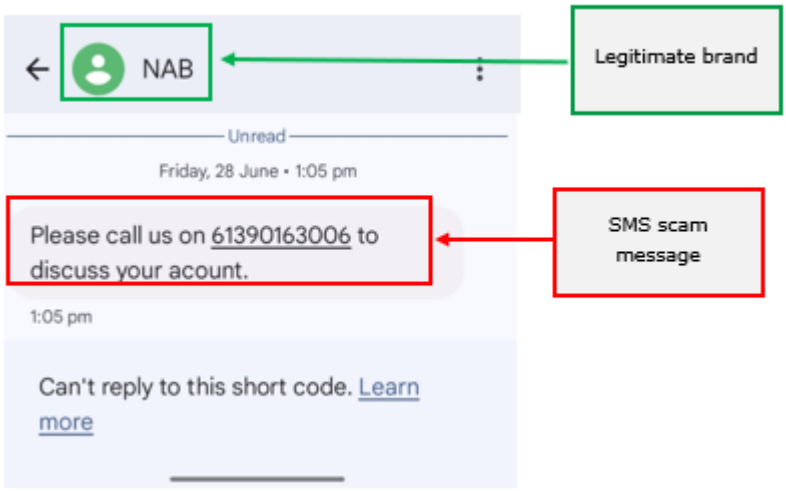
1.1 Impact of SMS scams

Australians lost $2.7 billion to scams in 2023.[i] SMS scams were associated with $27 million of those losses.[ii] The number of reported SMS scams has grown sharply at an annual rate of 28% over the last three years, rapidly becoming a significant concern for Australians.[iii] Outpacing email and phone scams, SMS is now the most common communication method used by scammers to target Australians. In 2023, Australians reported 109,600 SMS scams to Scamwatch, an increase of 37% from 2022.[iv] 13% of all scam victims report their incident to Scamwatch, however, the actual number of scams received is substantially higher.[v] The 2023 ACMA annual consumer survey revealed that 90% of Australians had received at least one scam text in the prior six months.[vi]

The number of SMS scams is driven in part by sender ID scams.[vii] For the purposes of this report, a sender ID is an identifier that consists of letters, or a combination of letters and numbers, which appear as the sender's name when a text message is received. In sender ID scams, scammers use sender IDs to impersonate legitimate businesses or government organisations to increase the likelihood a recipient will believe that the message is from a trusted brand, as shown in the example in Figure 1.1.

By using the same sender ID as the impersonated organisation, the scammer's texts can show up in the same text chain as previous legitimate texts. As a more sophisticated type of SMS scam that is harder to detect, sender ID impersonation scams pose significant risks to individuals and businesses. The consumer survey undertaken for this CBA found that 75% of people who receive SMS scams report receiving sender ID scams.

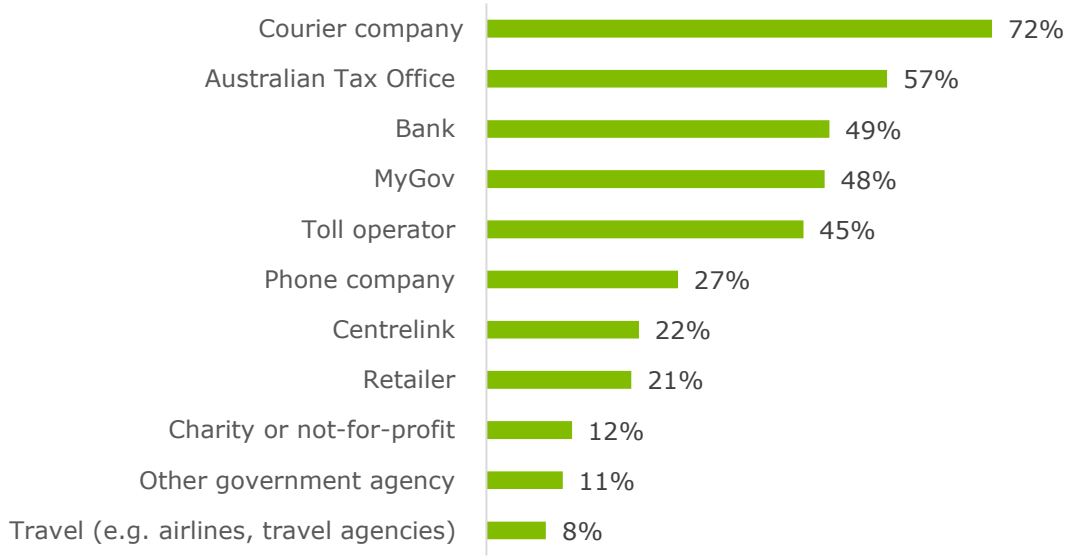
Figure 1.1: Example sender ID scam



Source: Deloitte Access Economics.

As sender ID messages only allow for one-way messaging which prevents recipients from replying, genuine use cases by legitimate organisations predominantly include transaction alerts, promotional messages, and service updates. Businesses and organisations may choose to use a sender ID to clearly identify themselves and reinforce brand identity in a bid to improve engagement with customers, or to reduce the likelihood that their messages will be marked as spam. The results of the Deloitte Access Economics consumer survey, which was conducted in August 2024, suggest that courier companies (e.g. Australian Post or DHL) were reportedly the most frequently impersonated organisations, followed by government services (Australian Tax Office and MyGov) and banks, as shown in Chart 2.1 below.[viii]

Chart 1.1 Types of organisations impersonated in scam texts



Source: Deloitte Access Economics analysis.

The financial harm caused by SMS scams can be considerable for both consumers and businesses. Individuals who report a scam are, on average, losing $246 for each incident.[ix] Beyond monetary losses, individuals incur time loss, trust erosion and impacts on psychological health. Where a scam leads to identity theft, victims can experience reputational damage and may be required to spend time resolving the issues caused by the compromise of their personal information.[x] Vulnerable groups, including culturally and linguistically diverse (CALD) communities, older Australians and Indigenous Australians, that are disproportionately impacted by SMS scams are likely to suffer high losses on average and encounter additional difficulties during recovery due to cultural or technological barriers.

Table 1.1 Differences in financial losses due 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)

Costs for spoofed businesses include decreased consumer confidence in their brand, time and money lost dealing with consumer complaints and reduced effectiveness of SMS as a communications or marketing channel. For example, a highly damaging sender ID scam received by HSBC customers resulted in broadly negative media coverage for the bank.[xi] The consumer survey revealed that 42% of consumers stop trusting sender IDs once they've received a scam SMS, and 46% are less likely to interact with legitimate texts from impersonated businesses and government agencies.[xii]

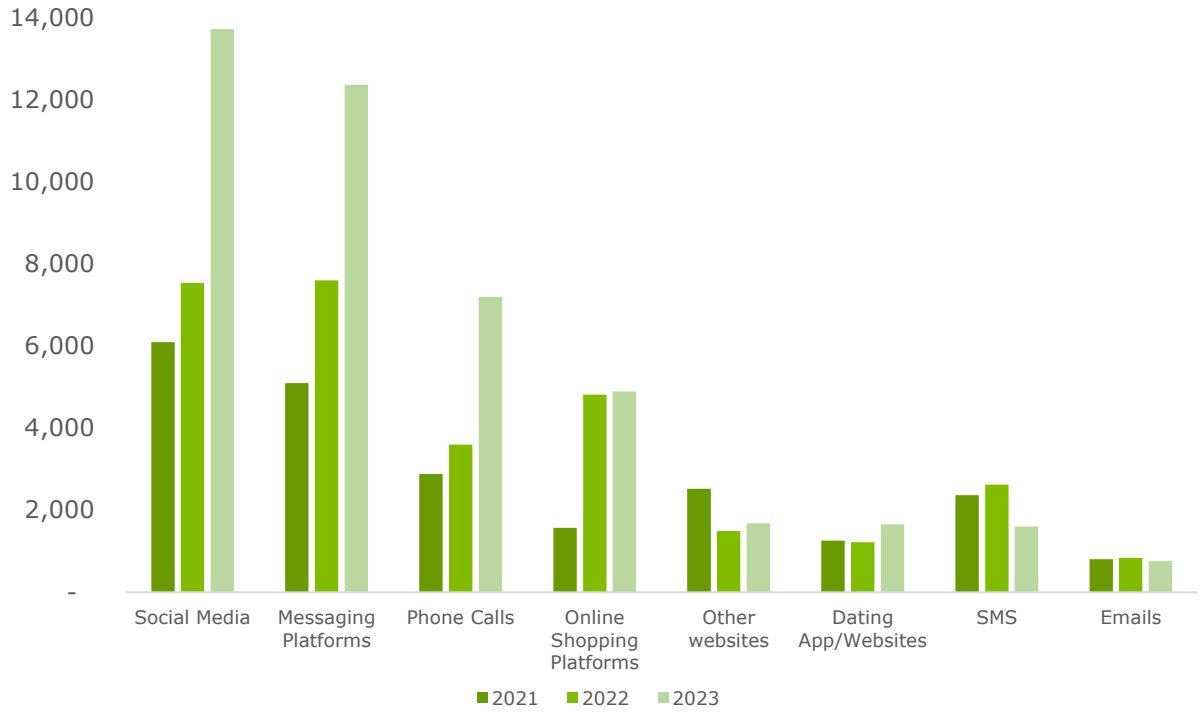
1.2 A Register can reduce harm

Introducing a sender ID register can provide another layer of protection for consumers and organisations, lessening the harm caused by sender ID scams. International evidence suggests that sender ID registration is effective at reducing SMS scams. For example, in Singapore, the Infocomm Media Development Authority has reported:

- the voluntary SSIR registration scheme implemented in March 2022 resulted in a 64% reduction in SMS scams from Q4 2021 to Q2 2022[xiii]
- the transition to the mandatory SSIR registration scheme in January 2023 resulted in SMS scams cases falling 70% in the three months after introduction compared to the three months before[xiv]
- however, Singapore's *Annual Scams and Cybercrime Brief 2023* reports reveals that, during the mandatory SSIR's first year of operation, total SMS scams only fell a total of 39% compared to the prior year – given the 70% initial decrease previously reported, the relatively lower rate of reduction suggests a possible pivot from scammers to using other methods of SMS scams.

While the Singapore register is broader than the potential register in Australia as it applies to short codes and numbers in addition to alphanumeric sender IDs (under either scheme), a key insight from the Singapore register is that scammers may switch to using other platforms to continue their operations. Chart 1.2 shows that social media, messaging platforms and phone calls have all experienced increases in reported scams in Singapore since the introduction of a register, although there is no evidence of a causal link to the introduction of a register. While increased scam activity on other platforms is a risk, it is relevant to note that harm is still reduced as scammers may find alternative platforms to be costlier and less effective for targeting consumers compared to SMS.

Chart 1.2 Contact methods used by scammers in Singapore



Source: Singapore Police Force.[xv]

Beyond Singapore, several other countries have established sender ID registers in response to rising SMS sender ID scam rates, as set out in Table 1.2. As more countries strengthen anti-scam measures, scammers will begin to target countries with fewer or less effective protections. Australia will become more vulnerable to scam efforts in the future if action is not taken to enhance current safeguards.

Table 1.2: International SMS sender ID registers

Country	Register design
United Kingdom	Commencing as an industry initiative through the Mobile Ecosystem Forum (MEF) in 2020, the Sender ID Protection Registry offers a voluntary registration scheme that allows organisations and government to protect their brand from fraudsters. Messages sent from entities that do not match the details registered against a sender ID are blocked. To protect brands, a block list is also maintained to ensure that sender IDs closely related to registered brands are not misused.
Singapore	The Singapore SMS Sender ID Registry (SSIR) was set up in March 2022 to enable organisations to protect their customers from receiving fraudulent SMS messages that spoofed the organisations' sender IDs. From January 2023 the SSIR transitioned to a mandatory registration scheme with all non-registered sender IDs being marked as "Likely-SCAM".

Country	Register design
Hong Kong	The Hong Kong SMS Sender Registration Scheme was established at the end of 2023 to help the public verify the identities of SMS senders. This scheme operates on a voluntary registration basis with a participating company or organisation having their sender ID sent with prefix "#". Rather than enabling fraudulent IDs to be identified or blocked, this enables legitimate senders to be clearly labelled for consumers.
Ireland	The Ireland SMS Sender ID Protection Registry launched in 2021 with participation from major government agencies, banks, retailers and utilities. The Irish Government has recently completed an assessment of future design, indicating an intention to move towards a mandatory registration scheme.

Source: Deloitte Access Economics.

1.3 Australian context

While efforts have been made to combat sender ID scams, there are several challenges that limit their efficacy.

Current anti-scam measures include the *Reducing Scam calls and Scam SMS Industry Code* (the Scams Code). The Scams Code includes a requirement that originating Carriers/Carriage Service Providers (C/CSPs) must only originate messages using an alphanumeric sender ID where the SMS sender has provided evidence that they have a valid use case for that sender ID.[xvi] Consultations with industry have indicated that the implementation of the Scams Code has had positive effects on reducing both phone scams and scam texts, though stakeholders report that compliance with the Scams Code has been inconsistent industry wide. In 2024, the ACMA found five telecommunication companies had failed to implement necessary checks to stop over 1.2 million scam texts from reaching customers during the period between 2022 to 2023.[xvii]

In April 2023, the Australian Government announced the planned introduction of a SMS Sender ID Register, aiming to reduce the frequency of SMS impersonation scams and increase protections for legitimate brands. The Register has been enacted through the *Telecommunications Amendment (SMS Sender ID Register) Act 2024* (the Act), which received Royal Assent on 5 September 2024.[xviii]

As an interim measure, the ACMA commenced a voluntary pilot register in December 2023. The pilot initially involved the consolidation and centralisation of existing arrangements that mobile network operators already had in place with certain organisations to protect their sender IDs from impersonation by scammers. The ACMA is in the process of expanding the pilot by invitation, to manage growth in the pilot phase and to make sure it operates as intended. Expansion is limited, however, as the pilot requires the registered sender ID to be originated by a single telecommunications company and these arrangements are not scalable. Alongside the pilot, individual telecommunication companies such as Telstra and Optus have been developing their own mechanisms to filter out SMS scams, often co-operating with key customers to protect specific sender IDs. However, stakeholder consultations have identified that the discrete protections provided by telecommunications companies are discretionary and limited in their effectiveness due to a lack of scalability, particularly when the message routing is complex. Additionally, as these scam protection measures are implemented at a cost to the telecommunication company and are unregulated, customers only receive enhanced protection at the discretion of the telecommunication company.

Efforts to reduce SMS scams therefore benefit from coordinated efforts to systematically curtail fraudulent activity. As acknowledged by telecommunications companies, a centralised mechanism like a register regulated and administered by a government body, would be a suitable design.

1.4 Purpose of this report

The Act, which received Royal Assent on 5 September 2024, establishes the framework for a SMS Sender ID Register and confers powers on the ACMA to develop and administer the Register but does not specify whether registration should be voluntary or mandatory.

The government's decision on whether the Register will be voluntary or mandatory is expected to be made by the end of 2024. The government consulted on the registration model in Q1 2024 and received submissions from industry participants and relevant stakeholders. The submissions have been used to support this report. This report has been prepared to inform the upcoming decision by providing an assessment of the impacts of both the voluntary and mandatory registration schemes.

1.5 Scope of the CBA

The Department has engaged Deloitte Access Economics to undertake a CBA of potential registration schemes to inform the establishment of a SMS Sender ID Register.

The following options are examined through the CBA:

1.5.1 Option 1 – Mandatory Registration

A mandatory registration scheme means organisations would need to apply to register any sender IDs used to send SMS to Australian mobile phones if they want to continue using those IDs without them being blocked or potentially labelled as 'likely scam' or similar. Telecommunications companies would be subject to enforceable rules (under an industry standard) under this scheme, whereby they would be required to block SMS with sender IDs or label them as 'likely scam' or similar unless they were registered and the sender is verified as the registered party. If an entity did not wish to register their sender IDs, they could use phone numbers as sender IDs instead, to avoid SMS being blocked or labelled as scams, or other forms of communication.

1.5.2 Option 2 – Voluntary Registration

A voluntary registration scheme would allow entities wishing to send messages with sender IDs to choose to apply to register those identifications. Telecommunications companies would be subject to enforceable rules requiring them to check registered sender IDs to determine whether the sender is the registered party, and block or label as 'likely scam' those that don't. Users with unregistered sender IDs would not be impacted by the Register.

2 Methodology

This section outlines the methodology and data sources underpinning in the CBA, including:

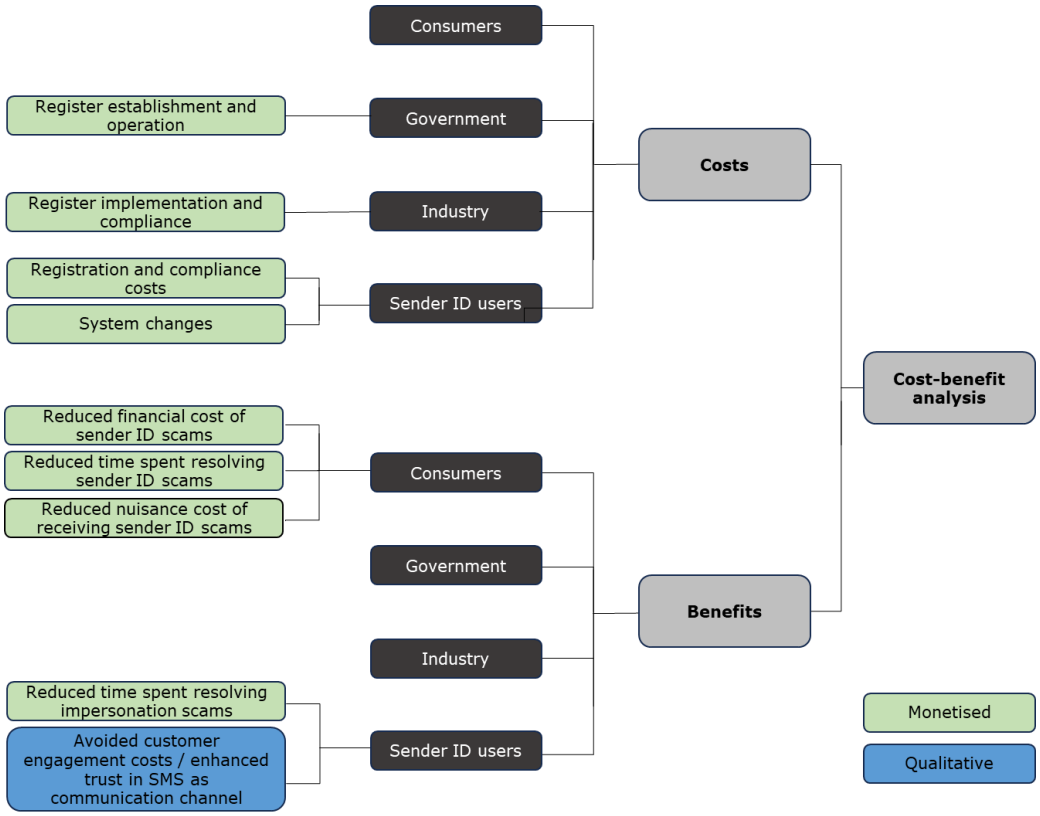
- modelling approach
- key costs and benefits defined for analysis
- policy options under consideration
- approach to data collection and validation
- limitations of the analysis.

2.1 Modelling approach

The intent of CBA modelling is to present a stylised forecast of the costs and benefits implied by certain actions – either taking place in real time or being considered for the future. The 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.

In this report, the CBA weighs the costs of the two SMS sender ID registration schemes against the benefits the schemes create. Costs and benefits are considered across four stakeholder groups – consumers, government, telecommunications industry participants and sender ID business users. Figure 3.1 provides a conceptual overview of the model structure that was used to define the categories of cost and benefit inputs for the CBA.

Figure 3.1: CBA model schematic tree



Source: Deloitte Access Economics.

The model calculates the relative costs and benefits of the options under consideration against the costs and benefits of a base case – a scenario in which neither option is implemented, and the status quo continues.

2.2 Key costs and benefits

This section outlines the costs and benefits to telecommunication industry participants, sender ID users, government and consumers. The costs and benefits for each group and policy option are considered, and a description of each cost and benefit is shown in Table 2.1.

Table 2.1: Costs and benefits considered through the analysis

Category	Stakeholder	Description	Quantified
Costs			
Register establishment and operation	Government	The costs associated with establishing and operating the Register including initial capital costs, onboarding sender ID registration and undertaking compliance and enforcement action.	Yes
Register implementation and integration	Telecommunication industry participants	The cost of amending internal processes or technology required to integrate with the Register and undertaking the blocking or tagging as fraudulent those sender IDs where the sender is not the authorised party.	Yes
Registration and compliance costs	Sender ID users	The internal resource cost of registering a sender ID and paying the applicable annual fee.	Yes
System changes	Sender ID users	The internal resource cost of implementation or varying systems for users with large numbers or complex arrangements for sender IDs use.	Yes
Benefits			
Reduced financial cost of sender ID scams	Consumers	The avoided financial losses associated with fewer sender ID scams received by consumers.	Yes
Reduced time spent resolving sender ID scams	Consumers	The avoided time spent resolving issues related to sender ID scams. This includes activities such as attempting to recover money lost, removing viruses or malware, and regaining access to online accounts.	Yes
Reduced nuisance cost of receiving sender ID scams	Consumers	The avoided cost or harm associated with receiving a reduced number of scam texts. Conceptually this includes the nuisance factor of receiving scam texts, time waste and loss of utility in SMS as a way of communicating.	Yes
Reduced time spent resolving customer complaints	Sender ID users	Reduced time spent resolving customer issues or complaints associated with having been impersonated via a sender ID scam text.	Yes
Avoided customer engagement costs / enhanced trust in SMS as communication channel	Sender ID users	Financial benefits associated with SMS being a more effective way of engaging customers including fewer missed appointments, improved ability to conduct marketing, and avoided costs engaging customers through other channels.	No

Source: Deloitte Access Economics.

2.2.2 Costs

Costs incurred by telecommunication industry participants are applicable to mobile network operators (MNOs), A2P SMS aggregators and A2P SMS retail providers who may participate in the Register. These costs are primarily associated with changing processes and systems to integrate with the Register, and ongoing costs to maintain systems that integrate with the Register. In addition, telecommunications industry participants will be required to block or tag as fraudulent those SMS with sender IDs that do not comply with the Register. For voluntary registration, this will involve blocking or tagging SMS for registered sender IDs where the sender is not the authorised representative or agent of the sender ID; for mandatory registration, this will mean blocking or tagging all unregistered sender IDs.

Government will incur costs establishing the Register, managing the registration process of sender IDs and maintaining the Register. However, as government intends to recover these costs through registration and annual fees, the impact will ultimately fall on sender ID users.

Costs incurred by sender ID users include the time and material cost of registering sender IDs and for implementing any necessary changes to internal processes required for the continued use of sender IDs. For example, understanding what sender IDs are currently in use across an organisation and establishing processes for their future use in customer communications.

Consumers are not expected to face any direct costs under the Register. 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. Given the uncertainty in ultimate impact, these second order effects are not considered. The distribution or final incidence of costs would also not change the total costs of each option and would, therefore, not change the CBA results or government's choice of preferred option.

2.2.3 Benefits

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

To the extent that receiving fewer sender ID scam texts is associated with consumers receiving fewer scam texts in aggregate, consumers also benefit from a reduction in the nuisances related to receiving scam texts. This includes the time wasted, confusion generated, or distress caused by receiving high volumes of scam texts. A reduction in nuisance is an intangible benefit and is not monetised within the CBA. However, qualitative impacts and an indicative magnitude of harm is presented based on parameters drawn from the literature.

Sender ID users will benefit from reduced costs associated with attempting to resolve issues related to scams through sender ID impersonations. This includes, consumers lodging complaints, attempting to retrieve or safeguard personal information, or restoring access to online accounts. Sender ID users also face costs associated with consumers reducing their engagement with communications sent via text. For example, reduced consumer engagement in text messages may adversely affect businesses because of consumers missing appointment reminders, experiencing more difficulty receiving customer's personal information, or incurring additional expenses due to engaging alternative communication channels to communicate with customers. The extent to which sender ID registration may improve consumers' trust and engagement with SMS is discussed qualitatively.

2.2.4 Period of analysis

This analysis considers the period from FY25 to FY35. As per the Office of Impact Assessment's (OIA) guidance, a timeframe of 10 years is utilised as the default period of analysis.[xix] The analysis considers the time required to establish the Register (which is expected to be operationalised by the end of 2025) and its on-going operation across the remaining period of the 10-year timeframe.

2.2.5 Data collection

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

Primary data collection

Surveys were developed and distributed to both business and consumers with review and approval from the Department. The surveys received a total of 618 responses from organisation (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
- '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:

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

Targeted consultations with telecommunication 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 qualitative findings from the pilot.

Further information on the surveys and consultations is detailed in Appendix B.

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 to potential impact of a register in Australia. Data on the number, characteristics and average losses from SMS scams were primarily informed from available Scamwatch public data.

2.3 Policy options

The two registration schemes are assessed against a base case – the status quo – where there is no Register and sender ID scam prevention is comprised of the existing protections in place under the Scams Code.

A summary of each policy option is outlined in section 1.5 of this report. The types of costs and benefits are the same under each option; however, the extent of sender ID registration and impact on scam communication differs between options.

2.4 Data cleaning, transformation and assumptions

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, which are summarised in Table 2.2. The full list of inputs and assumptions used in the CBA is detailed in Appendix A.

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 undertakes several validation processes including removing responses that complete the survey under a threshold length of time and those that consistently answer the same option across every question.

In line with standard approaches to statistical analysis, observed outliers in the data have been removed where the data is seen to be a result of data entry error or misunderstanding of the question, or where inputs are disproportionately high or low. Additionally, to appropriately use the observed data sets, the use of medians has been applied where appropriate to manage the skewed distribution of results.

2.4.1 Cost inputs

Key costs relate 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 IDs 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 is undertaken on these inputs.

2.4.2 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 under each policy option 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. These are reported in Section 3.5

Table 2.2: Key data used in the CBA

Source	Description of data
Organisation survey	Deloitte Access Economics (with the support of market research firm Dynata) conducted a survey of Australian businesses. The survey results informed the sender ID user benefit inputs used in the CBA. In total, there were 618 responses to the organisation survey (of which 150 were current sender ID users).
Consumer survey	Deloitte Access Economics (with the support of market research firm Dynata) conducted a survey of Australian consumers to understand the prevalence and impact of sender ID scams. The survey results informed many of the benefit assumptions used in the CBA. In total, there were 1,011 responses to the consumer survey.
Stakeholder consultation	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. A list of those consulted can be found in Appendix B.
Literature	Existing reports on the scam activities in Australia and overseas informed the development and validation of benefits. These include the ACCC's *Targeting scams: report of the ACCC on scams activity 2023* and research conducted through Ireland's Commission for Communication Regulation's *Combatting scam calls and texts Report* and consultation.
Office of Impact Analysis, Regulatory Burden Measurement Framework and CBA guidance note	The analysis adopts a 7% discount rate as recommended in the guidelines. The analysis also adopts the guidelines and recommendations for the value of productive staff time at $48.67 plus a multiplier of 1.75 to account for the non-wage labour on-costs (for example, payroll tax and superannuation) and

Source	Description of data
	overhead costs (for example, rent, telephone, electricity and information technology equipment expenses).

Source: Deloitte Access Economics (2024)

2.5 Interpretation and limitations

Two headline figures reported in this CBA are the NPV and the BCR.

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.

The BCR considers scale of benefits relative to costs, like a return to investment. For example, a BCR of 0.5 can be read as 'for every dollar of costs incurred as a result of the modelled change, you receive 50 cents of benefits in return'. A BCR of 1.5 on the other hand implies that 'for every dollar of costs incurred as a result of the modelled change, you receive $1.50 of benefits in return'. The larger the BCR, the greater the anticipated return to the modelled scenario.

While telecommunication industry participants consulted expect costs to be relatively small under either policy option, costs will ultimately depend on the technical design. However, as stakeholders report that costs are likely to be comparable under either option, uncertainty may impact the level of costs but not ranking of the options.

3 Analysis and results

This chapter presents the result of the analysis, including:

- primary results of the CBA
- sensitivity analysis on key modelling variables.

3.1 Primary results

The CBA indicate that the Register results in a BCR of 1.60 under the mandatory registration scheme (Option 1), while the voluntary registration scheme (Option 2) results in a BCR of 1.22. Under both options the benefits from avoided SMS sender ID scams outweigh the costs. The results for both options are presented in Table 3.1 and more detailed analysis of each cost and benefit and the underlying assumptions are discussed below.

Table 3.1: CBA calculation for the two options, NPV over 10 years at a 7% discount rate

	Option 1 (Mandatory registration)	Option 2 (Voluntary registration)
Costs ($ million)		
Government	20.5	20.5
Sender ID users	127.3	126.6
Industry	13.8	13.8
Total costs	**161.5**	**160.8**
Benefits ($ million)		
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**
Net benefits ($ million)	**96.2**	**35.2**
BCR	**1.60**	**1.22**

Source: Deloitte Access Economics analysis. Note: figures may not sum due to rounding.

3.2 Harms from sender ID scams

To understand the extent of potential benefits available under the policy options, the current level of harm associated with sender ID scams is estimated. This represents the maximum potential benefits that could be achieved if all sender ID scams were prevented. Each option is estimated to achieve a portion of the potential benefits based on the proportion of sender ID users that register under each option.

The total harms are outlined in Table 3.2, with details and additional qualitative benefits discussed in the following sections.

Table 3.2: Total monetised harm associated with sender ID impersonation scams

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

Source: Deloitte Access Economics analysis. Note: figures may not sum due to rounding

These values reflect the extent of harm in 2023. The trajectory of sender ID scams under the base case will therefore determine the potential level of annual harm in future years. In recent years, growth in SMS scams has been significant with volumes increasing by 28% since 2021 and reported financial losses increasing 63%. However, the introduction of the Scams Code may be contributing to a reduced impact of SMS scams with 2024 year-to-date financial losses down 57% compared to last year.

While recent trends may suggest the volume of 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 whether the current level of harm may be the extent of any reduction that can be attributed to other interventions. The central case of the CBA assumes a modest 5% annual growth in the volume of scams under the base case, with sensitivities presented in Section 3.6.

Each of the harms outlined in the above table are now considered in further detail.

3.2.2 Financial cost of sender ID scams

Financial losses for consumers from sender ID scams are the largest individual harm. While there are no available data on sender ID scams, Scamwatch reported 109,000 SMS scams corresponding to approximately $27 million in financial losses in 2023.[xx] 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'. Of those, 50,062 reported scams involved 'impersonation'. While these figures do not indicate how many SMS impersonation scams were specific to sender IDs, they provide insights into how pervasive SMS impersonation scams are.

To estimate the number and financial cost of sender ID scams specifically, the 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. 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 the 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.[xxi] To account for unreported scams, the 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).

Based on the parameters discussed above, the CBA model estimates that the total financial losses related to sender ID scams in 2023 was $26.6 million across approximately 108,000 scams.

3.2.3 Time spent resolving sender ID scams

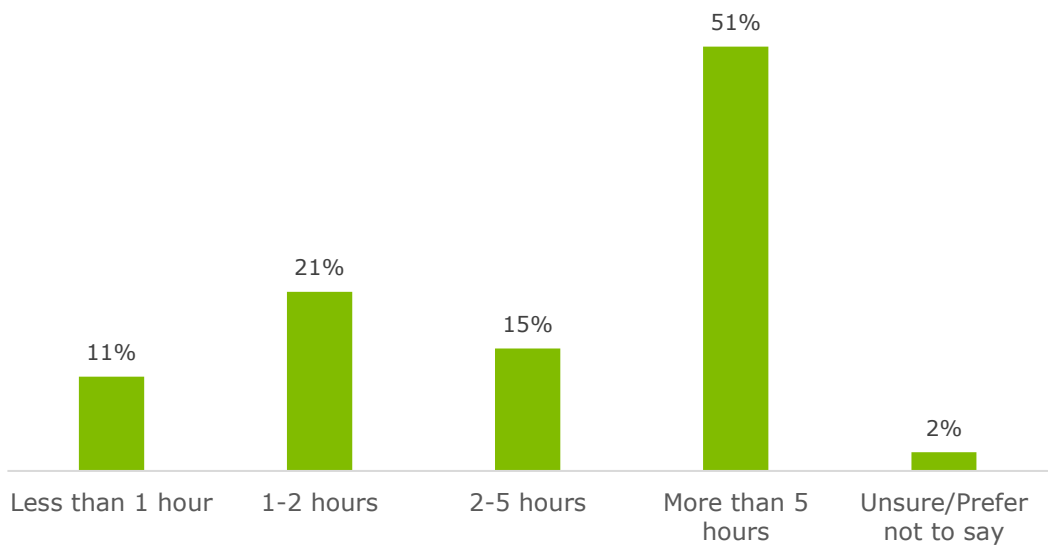
In addition to financial costs associated with scams, consumers face costs (in terms of time spent) related to resolving issues such as attempting to recover financial losses, changing passwords and regaining access to online accounts. These issues are common with 85% of consumers being scammed via SMS reporting that they encounter other issues (Chart 3.1).

Chart 3.1: Which issues (other than financial loss) did you encounter because of being scammed over text?

Source: Deloitte Access Economics consumer survey (2024)

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. This is likely a conversative estimate with over half of consumers spending more than the maximum amount of time listed in the survey (more than 5 hours) resolving issues.

Chart 3.2: How much time did you spend trying to resolve issues cause by the scam text?



Source: Deloitte Access Economics consumer survey (2024)

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.[xxii]

3.2.4 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. The 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, it can be estimated based on consumer's willingness-to-pay (WTP) to not receive SMS scams. Work commissioned by ComReg in Ireland undertook WTP experiments to elicit the value consumers place on being free from SMS scams.[xxiii] 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.[xxiv] 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 scam ($3.9 million).

3.2.5 Time spent resolving customer complaints

SMS impersonation scams impose costs on legitimate organisations because of consumers contacting these organisations to resolve issues such as recouping money, safeguarding data or recovering access to online bank accounts. The consumer survey suggests that consumers spent at least 295,000 hours in 2023 attempting to resolve issues. It naturally follows that at least some of this time would impose a corresponding burden on organisations.

To estimate the cost imposed on impersonated organisations, the 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). While data captured through the organisation survey and industry consultations undertaken as part of this CBA indicate that as many as 250,000 organisations are currently using sender IDs, 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.

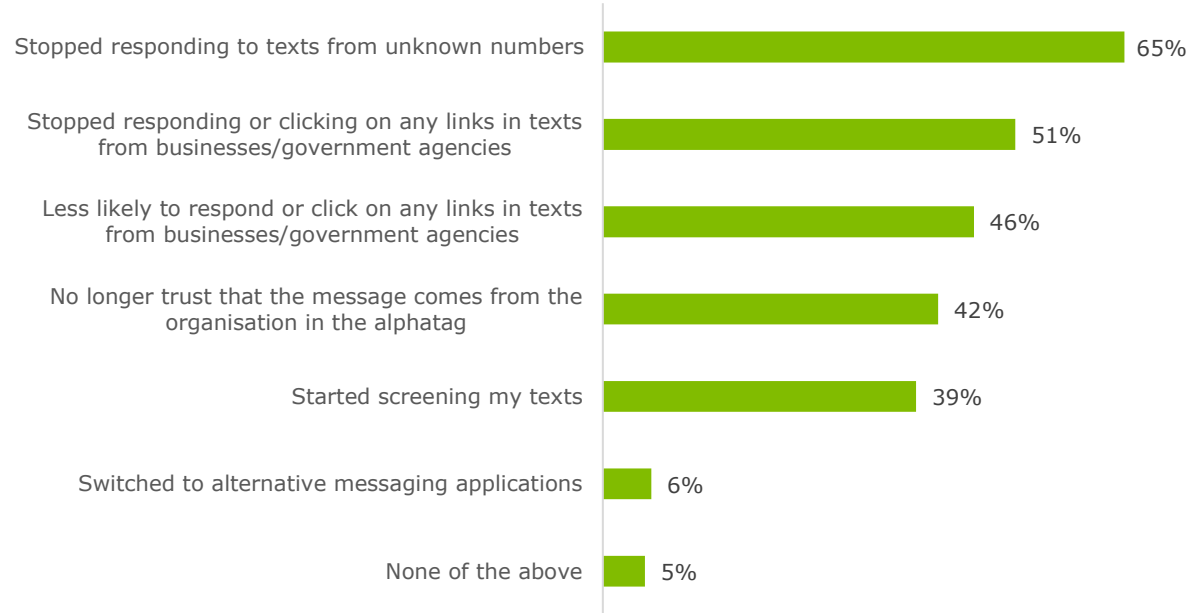
Based on these inputs, Australian organisations spend approximately 174,000 hours on responding to consumer issues related to sender ID impersonation scams, amounting to a time cost of $14.9 million in 2023.

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. The 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.

3.2.6 Loss of trust in SMS as a communication platform

SMS scams risk the utility of SMS as a communication platform. The 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 (Chart 3.3). Additionally, SMS as a platform is negatively affected with 84% of consumers agreeing that scam texts have reduced their level of trust in text messages as a way of communicating with others.

Chart 3.3: Share of consumers reporting changing behaviour in response to SMS scams



Source: Deloitte Access Economics consumer survey (2024)

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%)
- customers attending appointments/bookings (43%).

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, 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.[4] This benefit has not been included in the BCR due to a high degree of uncertainty in the extent of harms reduction that may be realised under each registration scheme. Additionally, it is unlikely that every dollar of harm reflects forgone revenue, with other impacts including late payments and issues receiving customer information.

3.3 Alphanumeric sender ID use and registration

An estimated 300,000 sender IDs are currently utilised in Australia. These users capture a broad range of users from government departments, large business, sole traders, community organisations and individuals. Some users may utilise A2P platforms operated by MNOs and aggregators, while other use sender IDs through technology products such as point of sale systems, customer relationship management products or other technology solutions. Some small users may have limited awareness that they are using sender IDs or that they differ from phone numbers.

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 telecommunication 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.

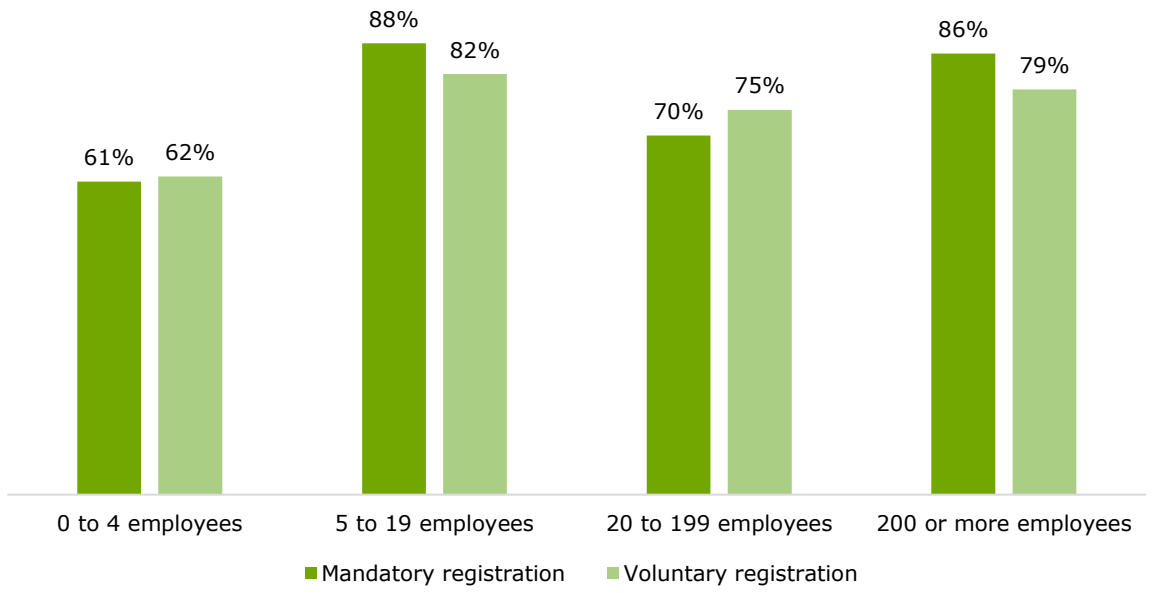
Registration intentions are estimated through the organisation survey by asking respondents whether they would register under each policy option. The results find similar rates of registration among current sender ID users with 78% indicating they would register under a mandatory registration scheme and 75% 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

[4] 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.

uncertainty of inputs, a sensitivity analysis has been conducted on the percentage of business registrations.

Chart 3.4 outlines registration intentions by employment size of survey respondents. It demonstrates that smaller organisations are less likely to register than larger organisations under both options. However, the share of smaller organisations' registration may be understated by the survey, as only a limited number of responses from smaller organisations using sender IDs were captured. In contrast, stakeholders consulted in the telecommunication industry indicated that the largest volume of sender IDs were associated with smaller organisations.[5] As such, a lower and constant rate of registration was assumed for these users with the survey not finding material differences in registration intentions.

Chart 3.4: Registration intentions by sender ID user organisation size



Source: Deloitte Access Economics organisation survey (2024)

Based on inputs from stakeholder consultations and the organisation survey, the estimated number of sender ID users by segment and corresponding registration intention by option are outlined in Table 3.3 below.

Table 3.3: Sender ID registration rates

	Potential registrants	Registration rate (Mandatory registration)	Registration rate (Voluntary registration)
High volume	500	78%	75%
Medium volume	22,000	78%	75%
Low volume	240,000	50%	50%

Source: Deloitte Access Economics (2024)

[5] One explanation for this outcome is that many smaller organisations may incidentally use sender IDs through a technology platform without identifying as a user.

3.4 Costs

This section outlines the costs faced by stakeholders. 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)
- sender ID user costs are assumed to commence from the start of 2026 (financial year 2025-26).

3.4.1 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 (e.g., NyGov, MyG0V or My Gov). 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 3.4: 2023-24 budget allocation

	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)

3.4.2 Telecommunication industry participants

Telecommunications industry participants are expected to incur an initial cost upon the creation of the Register and smaller ongoing compliance 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 CBA assumes that 30 SMS aggregators incur costs, which is the estimated number of Tier 1 aggregators (those with an existing relationship with an MNO). 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 register with the ACMA or a contracted Register administrator).

The MNOs consulted for this report were asked to estimate these costs and advised that they currently undertake many business processes aimed at blocking sender IDs 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. 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 the options.

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

Table 3.5: 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)

3.4.3 Sender ID users

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 register to become an approved user before registering each sender ID. The process outlined in the legislation is straightforward and is anticipated by the ACMA to require only moderate input.

Input from telecommunication industry participants suggest that some organisations may face additional complexity registering. The complexity arises due to organisations using multiple sender IDs or those organisations using complex arrangements and therefore needing to develop an understanding of how sender IDs are currently used across their organisation. On the other hand, pre-existing obligations under the Scams Code for originating C/CSPs to confirm that user has a valid use case for a sender ID likely necessitates similar, albeit less intensive, activities to be undertaken in the base case.

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. The estimated per user cost of registration is outline in Table 3.6 below.

Table 3.6: Sender ID user costs of registration

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

Source: Deloitte Access Economics (2024)

Based on the user registration rates outlined in Section 3.3, the total compliance cost (in terms of system change costs and administrative costs to register) across each option is outlined in Table 3.7 below. The costs are comparable due to the similar registration rates expected across the options. 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 either option.

Table 3.7: Sender ID user costs

	Option 1 (Mandatory registration)	Option 2 (Voluntary registration)
Systems change costs	2.0	1.9
Administrative cost, initial ($ million)	29.3	29.1
Administrative cost, renewal ($ million)	17.6	17.5

Source: Deloitte Access Economics (2024)

3.5 Benefits

The harms related to sender ID scams are disproportionately associated with the trusted brands who are currently experiencing impersonation (see Section 1.1). As such, the share of total current harms (outlined in Section 3.2) 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 level of protection under the voluntary registration scheme 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. As such, it was assumed that the voluntary registration scheme would be 80% as effective as the mandatory registration scheme, resulting in a 20% adjustment to benefits. This adjustment may be conservative as engagement with overseas regulators operating similar registration registers reported limited benefits associated with voluntary registration.

The effectiveness of both options in reducing scams in aggregate is also dependent on the response of scammers. For example, Singapore's scam data reveals that while 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 to defraud Australians, the CBA incorporates a five percentage point annual decrease in the effectiveness of both options.

The inputs used and results are summarised in Table 3.8 below.

Table 3.8: Total benefits, NPV over 10 years at a 7% discount rate

Harm	**Option 1 (Mandatory registration)**	**Option 2 (Voluntary registration)**
Effectiveness rate	78%	75%
Annal benefit decrease	5 p.p.	5 p.p.
Option effectiveness adjustment	-	- 20%
Avoided financial cost on scams	117.1	89.1
Reduced time spent resolving scams	61.7	46.9
Avoided nuisance cost	13.5	10.3
Avoided costs of resolving impersonation scams	65.4	49.7
Total benefit ($ million)	**257.7**	**196.1**

Source: Deloitte Access Economics analysis. Note: figures may not sum due to rounding

3.6 Sensitivity analysis

To understand how robust the results of this CBA are, sensitivity analysis was undertaken on a range of variables. Sensitivity analysis provides information about how changes in different variables will affect the overall costs and benefits of each option assessed. This analytical approach can be used to show how sensitive predicted net benefits are to different values of key variables and to changes in underlying assumptions.

As outlined above, the modelling results are most sensitive to a range of key inputs. These inputs are:

- Average financial loss per SMS sender ID scam

- The trajectory of scam growth
- Sender ID user registration rates
- Period of analysis
- Discount rates

Across all sensitives tested, the mandatory registration scheme receives a higher BCR than the voluntary registration scheme.

3.6.1 Average loss per SMS sender ID scam

The results are sensitive to the dollar amount that is attributed to avoided financial losses from scams, which is a significant driver of benefits under both options. To assess the results of the CBA under different average financial losses per SMS sender ID scam, the following percentages changes have been used for sensitivity testing:

- Average SMS financial loss year-to-date in 2024 ($119.84)
- Average SMS financial loss in 2022 ($357.75)

Table 3.9: Sensitivity analysis specific to average SMS losses (NPV terms over)

	Option 1 (Mandatory registration)	Option 2 (Voluntary registration)
Average SMS financial loss year-to-date in 2024 ($119.84)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	197.7	150.4
BCR	**1.22**	**0.93**
Base average financial loss ($246.00)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	257.7	196.1
BCR	**1.60**	**1.22**
Average SMS financial loss in 2022 ($357.75)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	310.9	236.5
BCR	**1.93**	**1.47**

Source: Deloitte Access Economics analysis. Note: figures may not sum due to rounding.

Table 3.9 shows the impact that varied average financial losses have on the overall BCR. The results demonstrate that the mandatory registration scheme is robust to both increases and decreases in average financial loss per scam, resulting in a BCR of greater than one under all scenarios. In contrast, the voluntary registration scheme results in a BCR of less than one when the average financial loss per scam is lower.

3.6.2 Growth in SMS scams

The results are sensitive to the trajectory of SMS sender ID scam growth under the base case, as it directly relates to the pool of potential benefits available. To assess the results of the CBA under different growth rates, the following percentages have been used for sensitivity testing:

- Lower scam growth (5% decrease in SMS scams annually)
- Higher scam growth (15% increase in SMS scams annually)

Table 3.10: Sensitivity analysis specific to scam growth (NPV terms over 10 years)

	Option 1 (Mandatory registration)	Option 2 (Voluntary registration)
Lower scam growth (5% decrease in SMS scams annually)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	165.7	126.3
BCR	**1.03**	**0.79**
Base scam growth (5% increase in SMS scams annually)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	257.7	196.1
BCR	**1.60**	**1.22**
Higher scam growth (15% increase in SMS scams annually)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	405.5	307.9
BCR	**2.51**	**1.91**

Source: Deloitte Access Economics analysis. Note: figures may not sum due to rounding.

Table 3.10 shows the significant impact of future growth in sender ID scams on the overall result of the CBA. The results demonstrate a sustained fall in the annual rate of scams result in the BCR of the voluntary registration scheme falling below 1. However, there is also significant upside potential if scams grow year-on-year.

3.6.3 Sender ID user registration rates

The results are sensitive to the dollar amount that is attributed to avoided financial losses from scams, which is a significant driver of benefits under both options. To assess the results of the CBA under different average financial losses per SMS sender ID scam, the following percentages changes have been used for sensitivity testing:

- Lower registration among low volume users (10% less than the central case)
- Higher registration among low volume users (10% higher than the central case)

Table 3.11: Sensitivity analysis specific to registration rates (NPV terms over 10 years)

	Option 1 (Mandatory registration)	Option 2 (Voluntary registration)
Lower registration among low volume users (10% less)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	257.7	196.1
BCR	**1.85**	**1.41**
Base registration among low volume users (50%)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	257.7	196.1
BCR	**1.60**	**1.22**
Higher registration among low volume users (10% more)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	257.7	196.1
BCR	**1.41**	**1.07**

Source: Deloitte Access Economics analysis. Note: figures may not sum due to rounding.

Table 3.11 shows the impact that the share of low volume sender ID users who register under either option has a significant impact on the overall result. For example, 10% lower registration raises the BCRs for the mandatory and voluntary registration schemes (1.85 and 1.41 respectively) while 10% higher registration reduces the BCRs for the mandatory and voluntary registration schemes (1.41 and 1.07 respectively). The relationship is due to a change in low volume registrations impacting costs but not the profile of benefits, as the risk of harm is predominantly concentrated among large, trusted users of sender IDs.

3.6.4 Five-year evaluation period

The telecommunications market is a fast-evolving sector with new technologies having the potential to change the relevancy of SMS a scamming method. For example, the introduction of Rich Communications Services (RCS) and other over-the-top (OTT) solutions may see a shift away from SMS.[xxv] While the legislation has mechanisms to capture new technologies in the future, the introduction of new communication methods could shorten the useful life of the Register.

To assess the results of the CBA timeframes, a shorter evaluation period of 5 years was used.

Table 3.12: Sensitivity analysis specific to average SMS losses (NPV terms over)

	Option 1 (Mandatory registration)	Option 2 (Voluntary registration)
Base evaluation period (10 years)		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	257.7	196.1
BCR	**1.60**	**1.22**
Shorter evaluation period (5 years)		
Total costs ($ million)	96.2	95.8
Total benefits ($ million)	121.9	93.5
BCR	**1.27**	**0.98**

Source: Deloitte Access Economics analysis. Note: figures may not sum due to rounding.

Table 3.12 shows the impact of a shorter evaluation period lowers the BCR of both options, as there are relatively high implementation and administrative costs and no benefits in the initial years of the CBA. While the mandatory registration scheme remains above 1, the voluntary registration scheme falls just below 1.

3.6.5 Discount rate

As per OIA's guidance on CBA, sensitivity analysis was undertaken producing results with an assumed discount rate of both 3% and 10%, where the central scenario assumes a discount rate of 7%.

Allowing the discount rate to vary to both 3% and 10%, respectively, does not have a material impact on the NPV or BCR under either option, reflecting the relatively uniform distribution of costs and benefits over time.

The results of this sensitivity analysis are presented below in Table 3.13.

Table 3.13: Sensitivity analysis specific to the assumed discount rate (NPV terms over 10 years)

	Option 1 (Mandatory registration)	Option 2 (Voluntary registration)
Discount rate of 3%		
Total costs ($ million)	188.8	188.0
Total benefits ($ million)	312.8	237.5
BCR	**1.66**	**1.26**
Discount rate of 7%		
Total costs ($ million)	161.5	160.8
Total benefits ($ million)	257.7	196.1
BCR	**1.60**	**1.22**
Discount rate of 10%		
Total costs ($ million)	145.2	144.6
Total benefits ($ million)	225.1	171.3
BCR	**1.55**	**1.19**

Source: Deloitte Access Economics analysis. Note: figures may not sum due to rounding.

Table 3.13 shows how the results vary by the discounts rates required by OIA. There are only minor differences in the BCRs across sensitives, indicative that the timing of costs and benefits do not play a material role in the results under the central case.

3.7 Regulatory burden estimates

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 outlines in Table 3.14 below. 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 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.

Table 3.14: 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
Mandatory registration	1.7	19.8	-	21.5
Voluntary registration	1.7	19.7	-	21.4

Source: Deloitte Access Economics analysis. Note: figures may not sum due to rounding.

4 Conclusion

The CBA suggests that the Register will generate significant benefits for consumers by reducing the costs associated with SMS sender ID scams. The benefits are highest under the mandatory registration scheme because under voluntary registration, unregistered users can still send SMS sender ID scams, resulting in costs to the economy. Consumers receive $192 million in benefits from avoided financial costs and avoided time spent resolving scams under the mandatory scheme, while sender ID users receive $65 million in benefits.

The costs of the Register are significant under both options. While government and telecommunication providers face relatively modest costs, sender ID users face approximately $127 million in administrative costs under both registration schemes. Business costs are primarily driven by a large volume of smaller businesses that face compliance costs (in terms of time and effort) to register. As such, the analysis indicates that the costs to sender ID users across the whole-of-economy exceed the estimated benefits they receive.

The CBA indicates that the benefits outweigh the costs for both mandatory registration (Option 1) and voluntary registration (Option 2), with mandatory registration delivering a greater net benefit. However, the sensitivity analysis shows that the BCRs are sensitive to changes in the volume and average financial loss associated with SMS scams.

The costs also vary depending on the timing of any requirement to register. The CBA calculations assume sender ID users register by the end of 2025, which is when the Register is anticipated to commence operations. However, it is anticipated that while the Register could be expected to be operational by late 2025, such commencement may involve entities submitting and registering their sender identifications during a transition period, prior to the Register being fully operational. As such, economy-wide upfront costs are highest in that year. After that year, costs are primarily driven by the administrative cost of undertaking annual renewals. If renewals where less frequent, costs would also be reduced.

Survey results suggested variation in sender ID user costs were dependent predominantly on the volume of users rather than user type. This reflects the large number of sender ID users who will incur small individual costs under either option. As the risk of sender ID scams are concentrated among larger and trusted brands, the registration of smaller sender ID users drives costs but not benefits.

The benefits estimated within the CBA only reflect those that can be monetised and quantified. Other benefits have also been reported, including the impact that increasing trust in SMS as a communications channel may have on sender ID usage. This benefit may be substantial with calculations suggesting the harms are as large as $7.8 billion in affected revenue annually due to missed appointments, late payment from customers and forgone revenue due to issues contacting customers. This benefit has not been included in the BCR due to a high degree of uncertainty in the extent of harms reduction that may be realised under each registration scheme.

The data captured through surveys and stakeholder consultations indicates that both consumers and sender ID users support the introduction of the Register – which is expected to lead to continued and, potentially, enhanced use of sender IDs. Some industry participants, however, report concerns regarding the additional regulatory cost to users to become registered, specifically for smaller businesses, as well as the capacity of the telecommunications network to effectively implement the Register. The concerns raised emphasise the value in considering a transition period for implementation of the Register and for incorporating effective education and communication strategies, and ensuring the registration process is straightforward.

Based on these conclusions, this report provides insights into the potential costs and benefits of both registration schemes under consideration for the Register, which can be used to inform government's decision on the preferred approach. The results illustrate both the potential value that can be generated through the introduction of a Register and the need to appropriately consider how any new regulatory requirements are implemented and enforced.

Appendix A Assumptions and sources

A.1. Assumptions

A.1.1. Number of sender ID users

It is estimated based on industry consultation that there are 300,000 sender IDs in use across Australia. However, there is uncertainty around distribution and use of sender ID across different types of organisations.

Stakeholder input in consultations suggested at least 80% of sender IDs send messages infrequently or on a low volume basis. This implies at least 240,000 sender IDs are associated with low volume users. Conversely, a relatively small number of users comprise a high share of total IDs used and total message volumes. There are examples of large retailers utilising individualised sender IDs across their many hundred locations.

Sender ID users' response to the introduction of a Register will likely differ across these groups. As such, for the purposes of the CBA, sender ID users were segmented into three groups:

- **High volume users**: 500 trusted brands and government entities that use a larger number of sender IDs as 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.

The average number of sender IDs used across the segments was informed by the organisation survey which found that the median number of sender IDs used is 1, while the average is 2.5. These numbers were user for the low and medium volume users respectively. The number of high volume users was validated against data provided by an industry participant, however, should be considered indictive.

Based on the organisation survey and information provided by industry participants, the input assumptions used through the CBA are outlined in Table A.1 below.

Table A.1: Number of sender IDs

	Sender ID users	Average number of sender IDs used	Number of sender IDs
High volume	500	10	5,000
Medium volume	22,000	2.5	55,000
Low volume	240,000	1	240,000
Total	**262,500**	**1.1**	**300,000**

Source: Deloitte Access Economics (2024)

A.1.2. Benefits assumptions and inputs used in the analysis

Table A.2: 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)

Table A.3: 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**

Source: Deloitte Access Economics (2024)

Table A.4: 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 Australian adults 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

Description of input	Unit	Value	Source
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)

Table A.5: Time spent 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)

Note: On-costs account for non-wage labour costs (for example, payroll tax and superannuation) and overhead costs (for example, rent, telephone, electricity and information technology equipment expenses). Additionally, the number of sender ID users impacted is based on the number of high and medium volume users outlined in section A.1.1.

Appendix B Primary data collection

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 and consultations. Deloitte Access Economics engaged the market research firm, Dynata, to support in the development and distribution of online surveys.

Consultation with other relevant stakeholders was also undertaken to understand the broader impacts of the proposed changes. The consulted stakeholders represented the views of different segments within the industry.

Surveys

Surveys were developed in coordination with Dynata and the Department and were distributed by Dynata for responses from consumers and organisations. The total response to the surveys were:

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

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.

Survey questions

Survey questions were designed in coordination with Dynata and the Department and were used to capture information that related to frequency and impact of scams (for consumers) and WTP, and potential costs of implementing the requirements (for businesses).

Consumer survey questions covered:

- General information on gender, age, postcode, SMS use and SMS scams experiences
- Frequency and impact of scams, including the number of impersonation scams received, types of organisations impersonated, and other experiences related to being scammed
- Loss of time and money from SMS scams, as well as reporting habits
- Trust erosion because of receiving SMS scams

Organisation survey questions covered:

- General information on number of employees, revenue, industry, use of SMS, and reliance on SMS for business activity
- Frequency and impact of SMS scams overall
- Frequency and impact of SMS impersonation scams
- Impact of SMS scams on consumer engagement with business
- Support for a Register, including preference between voluntary and mandatory, and whether use of Sender IDs would be impacted
- Willingness to pay for either registration scheme of the Register
- WTP ranges were:
  - Up to $100
  - Up to $250
  - Up to $500

- Up to $750
- More than $750
- We would not register at any price

Survey responses

The below tables provide a summary view of the survey responses based on the business and consumer profiles.

Table A.6 Organisation survey responses by annual revenue

WTP	Number of organisations	Percentage of organisations
$0 - $49,999	53	9%
$50,000 - $199,999	51	8%
$200,000 - $1,999,999	105	17%
$2,000,000 - $4,999,999	70	11%
$5,000,000 - $9,999,999	67	11%
$10,000,000+	152	25%

Table A.7 Organisation survey responses by number of employees

Response	Number of organisations	Percentage of organisations
0 to 4	104	17%
5 to 19	109	18%
20 to 199	173	28%
200 or more	215	35%

Table A.8 Organisation survey respondents (that use Sender IDs), response to question: In your view, should registration by sender ID users by mandatory or voluntary?

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

Table A.9 Organisation survey respondents (that use Sender IDs), response to question: If fees were based on charging for each alphanumeric sender ID registered, how much would your organisation be willing to pay per sender ID per year under a voluntary scheme?

WTP	Number of organisations	Percentage of organisations
Up to $100	38	27%
Up to $250	37	26%
Up to $500	30	21%
Up to $750	16	11%
More than $750	1	1%
We would not register at any price	20	14%
Total	142	100%

Table A.10 Organisation survey respondents (that use Sender IDs), response to question: If fees were based on charging for each alphanumeric sender ID registered, how much would your organisation be willing to pay per sender ID per year under a mandatory scheme?

WTP	Number of organisations	Percentage of organisations
Up to $100	39	28%
Up to $250	38	27%
Up to $500	35	25%
Up to $750	7	5%
More than $750	1	1%
We would not register at any price	20	14%
Total	140	100%

Table A.11 Consumer survey responses by age group

Age range	Number of consumers	Percentage of consumers
18-24	137	14%
25-34	168	17%
35-44	201	20%
45-54	185	18%

55-64	144	14%
65-74	129	13%
75+	47	5%

Table A.12 Consumer survey responses by disability

Disability	Number of consumers	Percentage of consumers
Yes	183	18%
No	818	81%
Prefer not to say	10	1%

Table A.13 Consumer survey responses by State

State	Number of consumers	Percentage of consumers
ACT	20	2%
NSW	340	34%
NT	5	0%
QLD	192	19%
SA	84	8%
TAS	20	2%
VIC	258	26%
WA	92	9%

Table A.14 Consumer survey responses by Area

State	Number of consumers	Percentage of consumers
ACT	20	2%
Sydney	241	24%
Rest of NSW	99	10%
Darwin	5	0%
Brisbane	100	10%
Rest of QLD	92	9%

State	Number of consumers	Percentage of consumers
ACT	20	2%
Adelaide	70	7%
Rest of SA	14	1%
Hobart	13	1%
Rest of TAS	7	1%
Melbourne	202	20%
Rest of VIC	56	6%
Perth	83	8%
Rest of WA	9	1%

Table A.15 Consumer survey responses by gender

Gender	Number of consumers	Percentage of consumers
Female	514	51%
Male	493	49%
Non-binary	3	0%
Other	1	0%

Table A.16 Consumer survey responses, response to question: To what extent do you agree that a Register scheme which verifies that SMS using alphanumeric sender IDs are from legitimate entities would increase your level of trust in SMS as a way of communicating?

Response	Number of consumers	Percentage of consumers
Strongly agree	291	29%
Somewhat agree	425	42%
Neutral	201	20%
Somewhat disagree	23	2%
Strongly disagree	16	2%
Unsure/ prefer not to say	55	5%
Total	1,011	100%

Stakeholder consultations

A range of government and business stakeholders were consulted to help inform the CBA analysis and development of this report.

Other industry stakeholder groups were invited to participate in a consultation or provide a written submission but were unable to provide input due to time and capacity constraints.

The stakeholder submissions provided to the Department in response to the consultation paper, *'Fighting SMS Scams – What type of SMS sender ID registry should be introduced in Australia?'*, were also used to inform the CBA analysis and development of this report.

Endnotes

[i] Australian Competition and Consumer Commission, *Targeting Scams: Report of the National Anti-Scam Centre on Scams Activity 2023* (Report, April 2024) <http://www.accc.gov.au>.

[ii] Australian Competition and Consumer Commission, 'Scam Statistics', Scamwatch (2024) <https://www.scamwatch.gov.au/research-and-resources/scam-statistics>.

[iii] Ibid, Deloitte Access Economics analysis.

[iv] Ibid, Deloitte Access Economics analysis.

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

[vi] ACMA, 2023 ACMA annual consumer survey [data set], ACMA, Australian Government, (unpublished), accessed 10 September 2024. Question B11. In the past 6 months, how often have you received scam SMS?

[vii] Deloitte Access Economics, *Consumer Survey* (2024).

[viii] Ibid.

[ix] Australian Competition and Consumer Commission, 'Scam Statistics', Scamwatch (2024) <https://www.scamwatch.gov.au/research-and-resources/scam-statistics>.

[x] IDCARE, 'Unauthorised Mobile Phone Porting Events', IDCARE Insights Bulletin (2018).

[xi] ABC News, 'HSBC Customers Demand Action Against Spoof Scams' (8 March 2024) <https://www.abc.net.au/news/2024-03-08/hsbc-customers-demand-spoof-scam-action/103549516>.

[xii] Deloitte Access Economics, *Consumer Survey* (2024).

[xiii] Singapore Police Force, Annual Scams and Cybercrime Brief 2023 (Report, 2023) <https://www.police.gov.sg/-/media/8F06592D8FBE475C8D2B92EB3BFFE7FC.ashx>.

[xiv] Ibid.

[xv] Ibid.

[xvi] Communications Alliance Ltd, C661:2022 Reducing Scam Calls and Scam SMS (Industry Code, 2022) <https://www.commsalliance.com.au/__data/assets/pdf_file/0015/72150/C661_2022.pdf>.

[xvii] Australian Communications and Media Authority (ACMA), 'Five Telcos Breached for Allowing SMS Scams' (15 February 2024) <https://www.acma.gov.au/articles/2024-02/five-telcos-breached-allowing-sms-scams#:~:text=Investigations%20by%20the%20ACMA%20found,names)%20without%20sufficient%20checks%20to>.

[xviii] *Telecommunications Amendment (SMS Sender ID Register) Act 2024*.

[xix] Office of Impact Analysis (OIA) Cost-benefit analysis guidance note, Department of the Prime Minister and Cabinet (2020).

[xx] Australian Competition and Consumer Commission, 'Scam Statistics', Scamwatch (2024) <https://www.scamwatch.gov.au/research-and-resources/scam-statistics>.

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

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

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

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

[xxv] Australian Broadcast Corporation, Apple announces surprise adoption of RCS messaging, 'the new SMS' Android-maker Google spent years pushing for (17 November 2023) <https://www.abc.net.au/news/2023-11-17/apple-rcs-adoption-2024-messaging-android-google-sms/103117468>.

Limitation of our work

General use restriction

This report is prepared solely for the internal use of Department of Infrastructure, Transport, Regional Development, Communications and the Arts. This report is not intended to and should not be used or relied upon by anyone else, and we accept no duty of care to any other person or entity. This report has been prepared for the purpose of reporting on the cost benefits analysis of SMS Sender ID Register options. You should not refer to or use our name or the advice for any other purpose.

Deloitte.