Australian Government

acma

Australian Communications and Media Authority

Reducing the impact of scams delivered via short message service (SMS) Regulation Impact Statement

JUNE 2022

acma.gov.au

Canberra
Red Building
Benjamin Offices
Chan Street
Belconnen ACT

PO Box 78
Belconnen ACT 2616

T +61 2 6219 5555
F +61 2 6219 5353

Melbourne
Level 32
Melbourne Central Tower
360 Elizabeth Street
Melbourne VIC

PO Box 13112
Law Courts
Melbourne VIC 8010

T +61 3 9963 6800
F +61 3 9963 6899

Sydney
Level 5
The Bay Centre
65 Pirrama Road
Pyrmont NSW

PO Box Q500
Queen Victoria Building
NSW 1230

T +61 2 9334 7700 or 1800 226 667
F +61 2 9334 7799

Contents

Introduction

The Australian Government wants to prevent scams targeting users of telecommunications services, and support measures that mitigate fraud and associated harms to Australians.

Mobile devices often contain large amounts of personal information. They are regularly used for user-authentication for a range of accounts, including with telecommunications providers, financial and banking institutions, social media, retail websites and government services (such as the myGov online portal).

Bad actors (or scammers) are increasingly finding new ways to target business processes and technologies to perpetrate scams on and through telecommunications services. The scale and sophistication of the third-party bad actors causing the problem means industry, government and consumers must remain vigilant. This is an environment where scammers will ruthlessly test perceived and actual weaknesses in systems, processes, regulations and markets.

Scammers will also 'socially engineer' scam outcomes by continually testing and seeking to manipulate consumers and telecommunications providers. They perpetrate their crimes via a range of obfuscation techniques and scam activity, such as stealing someone's identity details or money via malicious hyperlinks delivered via short message service (SMS).[1]

The wide use of communications technologies – including essential telecommunications services – as a channel to a significant range of critical transactions and social interactions has increased consumer expectations. Those who access those technologies and services want them appropriately safeguarded from harms.

In 2020 and 2021, new rules were introduced to improve consumer safeguards and reduce instances of mobile porting fraud, scam calls and high-risk customer transactions. We are seeking to further improve safeguards by exploring options to reduce the impact of scam activity initiated via SMS.

Background

Regulatory setting

The ACMA is an independent Commonwealth statutory authority. We regulate communications and media services in Australia to maximise the economic and social benefits for Australia. This includes regulating telecommunications providers.

We regulate in accordance with 4 principal acts – the *Radiocommunications Act 1992*, *Telecommunications (Consumer Protection and Service Standards) Act 1999*, *Broadcasting Services Act 1992*, and the *Telecommunications Act 1997* (Telecommunications Act). We also have responsibilities under the *Interactive Gambling Act 2001,* the *Spam Act 2003* and the *Do Not Call Register Act 2006*.

[1] SMS is the text messaging service component of most telephone, internet, and mobile device systems. It uses standardised communication protocols that let mobile devices exchange short text messages – allowing users to send and receive messages of up to 160 characters (when entirely alpha-numeric) to and from Global System for Mobile Communications (GSM) mobiles.

Reporting and compliance
Multiple government and law enforcement agencies have statutory roles and/or receive reports of scam activity. The ACMA has a role to play as the sectoral regulator of the telecommunications industry, and for e-marketing and telemarketing.

Other key agencies with relevant regulatory responsibilities (and which receive scam reports from consumers) include the Australian Competition and Consumer Commission (ACCC) as the Commonwealth competition and consumer regulator, the Australian Cyber Security Centre (ACSC) as the Australian Government lead on cyber security issues, and the Australian Federal Police (AFP) and other law enforcement agencies in relation to perpetrated scams.

Provision of telecommunications services
Under the Telecommunications Act, 2 main types of organisations are involved in the provision of telecommunications services to the public – carriers (C) and carriage service providers (CSPs).[2] They play a frontline role in protecting their customers, keeping their networks secure and in phone scam disruption activities.

A carrier has complex infrastructure and systems. It owns network units that deliver carriage services. Its facilities may include transmission infrastructure, cabling, wireless networks and satellite facilities. Carriers have a large customer base and high traffic volumes. They operate international gateways that carry network traffic originating overseas and terminating in Australia.[3]

A CSP does not have its own network units – it provides telecommunication services over units that a licensed carrier owns, and network units covered by a nominated carrier declaration. A CSP can include organisations that resell time on a carrier network for phone calls, provide access to the internet (internet service providers) and provide phone services over the internet, referred to as Voice over Internet Protocol, or VoIP, service providers.[4]

Although not directly responsible for the harms and impacts caused by scammers, C/CSPs are responsible for the security of their networks and assisting to prevent the use of their services in the commission of an offence against the Commonwealth, state or territory.

Alignment with measures to reduce the impact of scam calls
In 2020, we conducted a regulatory impact analysis (RIA) to look at options to reduce the scale and impact of scam calls on Australians. The Regulation Impact Statement (RIS), *Reducing the impact of scam calls* (RISC RIS), recommended enforceable obligations as delivering overall net benefits of $17.2 million over a 10-year period. The RISC RIS was assessed by the Office of Best Practice Regulation (OBPR) as consistent with good practice in line with the Australian Government's requirements.

In December 2020, we registered new rules developed by the industry peak body Communications Alliance Ltd (Communications Alliance) requiring C/CSPs to detect, trace and block scam calls. In the first 16 months of the *Reducing Scam Calls* industry code (RSC code) being in force, more than half a billion scam calls were blocked,[5] significantly reducing the impact of scam calls on Australians.

[2] ACMA, 'About carriers and carriage service providers', viewed 28 March 2022.
[3] ibid.
[4] ibid.
[5] ACMA Media Release, 2022, *Scam crackdown results: Telcos block half a billion scam calls*, viewed 3 May 2022.

The analysis undertaken in the RISC RIS is also relevant to the analysis exploring the options to reduce the impact of scams delivered by SMS. In particular, the consideration of the:

- harms – financial loss, identity theft, psychological harm and emotional distress
- policy problem (and why government action is needed)
- options available to address the problem (status quo, consumer education campaigns, or enforceable obligations).

Regulatory framework

The legislative framework confers powers on the ACMA in the event industry codes fail to operate effectively or are not developed by industry. Under Part 6 of the Telecommunications Act, the options available to us to make obligations enforceable are either an industry code or an industry standard.[6]

We may call for an industry code to be made providing certain threshold conditions are met or register an industry code if submitted by a body representing the industry (if certain matters are satisfied). It may determine a standard where a code has been called for and not provided, where a code fails, or, where we are directed to make such an instrument by the minister administering the Telecommunications Act.

Placing obligations in an industry code provides the ACMA with initial enforcement powers to give formal warnings or directions to comply with the code. Civil penalties can then be pursued through the Federal Court or an infringement notice issued if a direction to comply is then breached (under Part 31 of the Telecommunications Act). If an industry code proves deficient, then an industry standard could be considered (section 125), including under ministerial direction (subsection 125AA (4) of the Telecommunications Act).

We also have powers to make a service provider determination under section 99 of the Telecommunications Act that applies to certain service providers in relation to the interests of customers.

If a standard or service provider determination is contravened, the ACMA may:

- issue a formal warning
- give a remedial direction
- accept an enforceable undertaking
- give an infringement notice
- seek an injunction in the Federal Court to compel the person to act or refrain from acting in a particular way
- seek civil penalties via Federal Court proceedings (up to $50,000 for a person and $250,000 for a body corporate per contravention).

[6] Part 6, *Telecommunications Act 1997*, viewed 15 June 2022.

This RIS covering scams delivered via SMS should be read as an extension that builds on the analysis undertaken on options to address scam calls. It incorporates existing information from the RISC RIS. However, where updated data is available or is specific to the problem of SMS scams, this RIS provides further analysis of the issue. For example, measures to reduce the impact of SMS scams rest more narrowly with CSPs that supply mobile services (mobile CSPs) or arrange for the supply of mobile carriage services (e.g., SMS aggregators[7]). Whereas measures to mitigate scam calls apply to carriers and CSPs that supply both fixed and mobile services.

[7] SMS aggregators are the gateway between carriers and text messaging software providers. Australian businesses can use a messaging gateway to send bulk text messages for alerts, marketing and communication campaigns or 2-way messages via a gateway network.

What is the policy problem?

Telephone numbers in connection with the supply of a telecommunications service have become a fundamental enabler of our digital identities. Mobile phones and other devices can also provide portable digital identity credentials capable of authenticating users for a variety of online and offline transactions.

The mobile phone has become an important device that we always have on hand. People use them to keep in touch with friends and family through voice calls, text messages, messaging applications and social media. Mobile phones remain by far our most popular communication device – 99% of Australians now use one, while nearly all of us own a smartphone (94%, up from 83% in 2019). More than twice as many people aged 75 and over owned a smartphone in 2021 compared to 2019 (76% up from 35%).[8]

Australian adults are also using their mobile phones beyond calling and messaging – including for activities such as navigating with GPS and proprietary maps, accessing news or audio content, and for multi-factor identity authentication to pay bills and access banking, emails, social media platforms, government services, education or retail accounts.

Numbers, phones, and other devices are valuable not only to the user but have also become prized assets for criminals or bad actors (scammers) to commit identity and financial theft and fraud. While scams can be perpetrated in any number of contexts, many Australians are exposed to scams via their communications services. The digital and telecommunications environments have provided attractive and generally low-cost, high-volume and high-anonymity channels for scammers to target.

Scammers will use an illegitimately obtained phone number (or service) to gain access to bank accounts, social media, online businesses, government services such as myGov and any other account that uses the phone as a secondary security check. If a scammer gains unauthorised control of a number or service, they can hijack identities, obtain financial benefit or fraudulently take control of Australians' digital lives.

Scammers perpetrating fraud via SMS

Since the first SMS was sent to a mobile phone in 1992,[9] SMS has become a popular communication channel. SMS is a universal technology supported by every mobile network and most devices. Recent ACMA research shows that 91% of Australians reported using their mobile phone for texting, second only to calls.[10] SMS – and Multimedia Messaging Service (MMS)[11] – can reach a recipient anywhere and at any time of the day where there is mobile coverage. All that is needed to start texting is another person's mobile phone number.

SMS is also a popular channel for businesses to communicate with customers because it is more immediate than email and does not require any additional application downloads. Text messages are used for informing customers about ongoing promotions, closing periods, schedule changes and upcoming sales. SMS for

[8] ACMA 2021, *Communications and media in Australia: How we communicate*, viewed 19 April 2022.
[9] TextMagic 2019, *The History of Texting: from Telegraphs to Enterprise SMS*, viewed 19 April 2022.
[10] ACMA 2021, *Communications and media in Australia: How we communicate*, viewed 19 April 2022.
[11] MMS includes multimedia content to and from a mobile phone over a mobile network and allows the exchange of text messages greater than 160 characters in length. Unlike text-only SMS, MMS can deliver a variety of media, including up to 40 seconds of video, one image, a slideshow of multiple images or audio.

transactional purposes are also highly valued by health professionals, lawyers and accountants who use them to confirm, move or remind clients of appointments.

Australians have become accustomed to receiving communications via SMS from businesses or organisations that they trust. People expect texts to be from people they know, or from institutions they've trusted with their mobile number. People are far more likely to fall for a scam using a specific or trusted brand if they've already received a genuine communication from the business or organisation. Psychologists refer to this feeling as 'illusory correlation', which happens when we see events as linked when they're not. Illusory correlation tends to confuse or relax our natural caution, making us more vulnerable to scams.[12]

SMS scams may:

- attempt to obtain financial or personal information (SMS phishing)
- download malicious code on a device (access hacking)
- impersonate trusted brands
- fraudulently vary or impersonate sender ID of a trusted organisation to add a layer of credibility.

Scammers seek to exploit vulnerabilities in the system as well as a consumer's trust in that channel. Many malicious campaigns use a scatter-gun approach, targeting thousands of phone numbers sequentially (such as by starting with '0400 000 000' and working up), randomly (with the aim of seeming less predictable), or using stolen lists of valid numbers.[13] And while most mobile devices do have options to block or filter numbers – such as by SMS filtering services or by categorising unknown numbers – much like email spam filters, these approaches are generally only as reliable as the data collected from user reports.[14]

Scammers perpetrate potential fraud attacks via abuse of SMS to try to get people to click on a link that could compromise their mobile phone or service, trick them into making an expensive phone call, or send a message which could cost them money. The aim is often to encourage people to respond on impulse rather than thinking through whether they may be being scammed.

[12] The Conversation 2021, *Why are there so many text scams all of a sudden?*, viewed 20 April 2022.
[13] The Conversation 2021, *Being bombarded with delivery and post office text scams? Here's why — and what can be done*, viewed 19 April 2022.
[14] ibid.

Many of the scams delivered by SMS are 'phishing' or 'smishing'[15] scams where scammers send 'deceptive messages … pretend[ing] to be from a large organisation you trust to make the scam more believable'.[16]

Source: *Targeting scams*, Australian Competition and Consumer Commission © Commonwealth of Australia 2021.

Phishing is a way that cybercriminals steal confidential information, such as online banking logins, credit card details, business login credentials or passwords and passphrases by sending fraudulent messages (sometimes called 'lures').[17] The messages entice recipients to click on links that draw them to maliciously controlled websites where either personal information is obtained or malware is unknowingly downloaded.

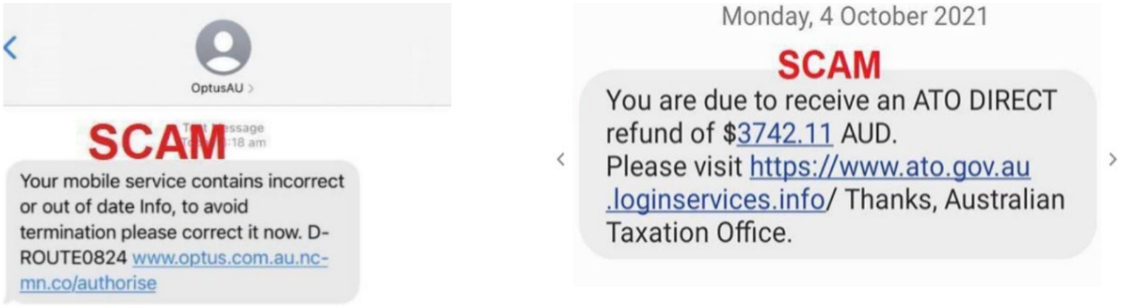
Scams delivered by SMS also use 'over stamping' or 'spoofing' sender IDs.[18] Spoofing, in scam terms, is the practice of disguising a scam communication to appear as though it came from a trusted source. Usually, scammers spoof a trusted organisation such as government agencies, banks, law enforcement or utility companies. Scammers replace or alter the originating mobile number (sender ID) of a text message (sent via SMS) to an alphanumeric text of their choice – in effect resetting the sender ID of an SMS to change who the sender appears to be. This can,

[15] 'Smishing' is the colloquial term for texting people while purporting to be legitimate but only seeking money or sensitive data or intending to wreak havoc with a computer device. The term marries 'short message service' (or SMS) and phishing.
[16] Australian Cyber Security Centre, *Phishing scams*, viewed 28 March 2022.
[17] ibid.
[18] A sender ID is a numeric or alphanumeric contact that identifies who has sent an SMS. Sender IDs appear at the top of text message conversations and help users recognise what organisation or business has sent a particular message. Sender IDs can be custom words, dedicated numbers or shared numbers.

due to the way platform applications work, permit an illegitimate message to slip into the message stream related to the legitimate entity – thereby providing a further measure of trust.

By impersonating a trusted organisation, the scammer is more likely to be successful when they send a message with a malicious hyperlink contained within the text, as the scam is supported by a measure of seeming legitimacy. If clicked on by the consumer, the hyperlink could link to a fraudulent site or install a piece of software on a mobile device – putting both personal information and the device at risk.

Examples of scams delivered via SMS



Source: Nine News 2022, Scams in Australia in pictures: Scams and hackers catching unaware Aussies out via email, online, phone texts and more.

Flubot scam

In 2021, Australians were increasingly targeted with SMS messages carrying the Flubot malware. This malicious software (malware) has migrated from Europe to Australia and sends text messages to both Androids and iPhones (with Androids more at risk).

In August 2021, the ACCC's Scamwatch reported the first instances of the Flubot scam in Australia. By October 2021, there had been over 16,000 reports of Australians getting scam text messages about missed calls, voicemails or deliveries.[19]

There are a large number of different types of Flubot text messages, and scammers are constantly updating them with the intention of stealing online banking credentials. They are delivered via SMS and attempt to convince the recipient they must install an 'app' on their smartphone to reschedule a missed delivery or listen to a fake voicemail or view photos that have been uploaded. Unfortunately, rather than an actual app downloaded from the app store, this fake app contains malware which is installed when the link in the SMS message is clicked.[20]

Once installed, the malware provides 'overlays' (fake pages) on top of the login screens of genuine banking apps installed on the phone. The next time the victim uses their real banking app, the overlays capture their banking details, which are then fed back to servers controlled by cyber criminals.[21]

Impact of scams on Australians

Scam activity impacts directly on the financial and emotional wellbeing of many Australians. It also undermines confidence in our telecommunications services and

[19] ACCC 2021, *Types of scams*, viewed 6 April 2022.
[20] The Conversation 2021, *Being bombarded with delivery and post office text scams? Here's why — and what can be done*, viewed 19 April 2022.
[21] ibid.

legitimate (consensual) marketing. In this sense, CSPs and the broader community (beyond victims of scams themselves) are also impacted by scam activity, even where they have not been directly involved in a scam.

Fraud

Fraud can be defined as 'dishonestly obtaining a benefit, or causing a loss, by deception or other means'. In this definition, 'benefit' refers both to tangible items, such as money or objects, and intangible benefits including power, status or information.[22]

The impact of fraud goes well beyond financial loss. Fraud impacts people, industries, entities, services and the environment. Understanding the total impact of fraud allows entities to make better informed decisions. Serious impacts can arise from any type of fraud, whether it's carried out by opportunistic individuals or serious and organised criminal groups. However, serious and organised crime can often increase the scale and impacts of fraud.

Fraud can be categorised by type or by the industry in which it occurs, including superannuation fraud, serious and organised investment fraud, mass marketed fraud, revenue and taxation fraud, financial market fraud, card fraud and identity fraud (discussed below).

Identity crime

Identity crime continues to be one of the most common crimes in Australia. According to the Australian Institute of Criminology (AIC), the annual economic impact of identity crime exceeds $2 billion.[23] The indirect cost of identity crime in 2018–19 was estimated to add a further $1 billion, bringing the total economic impact of identity crime in Australia for 2018–19 to approximately $3.1 billion.[24]

A survey by the AIC found that 1 in 4 Australians have been a victim of identity crime at some point in their lives. In 2020, Scamwatch reported that 25% of all scam reports involved the loss of personal information – up from 16% in 2019. The increasing value of personal information at a time when face-to-face interactions were not possible was a significant driver of scam activity in 2020.[25]

Identity crime can take many forms, including:

- the theft of personal identity information and related financial information
- assuming another person's identity for fraudulent purposes
- producing false identities and financial documents to enable other crimes.

Identity crime is also used in serious and organised crime. Fraudulent identities may be used for removing funds from bank accounts, money laundering, tax evasion, dealing in stolen motor vehicles, or to protect the true identities of organised crime members and travel without being identified or traced by law enforcement agencies.[26]

In addition to facilitating the commission of other offences, organised criminals may also sell stolen identity information to criminal networks. When a person has their identity stolen, they may experience repeated victimisation. In this way, organised

[22] Commonwealth Fraud Prevention Centre, (counterfraud.gov.au), viewed 20 April 2022.

[23] Identity crime and misuse in Australia (homeaffairs.gov.au), viewed 20 April 2022.

[24] Australian Institute of Criminology, 2020, *Identity crime and misuse in Australia 2019*, viewed 20 April 2022.

[25] ACCC 2021, *Targeting scams - a report of the ACCC on scam activity 2020*, viewed 7 April 2022.

[26] Attorney-General's Department, '*Fraud in Australia*', viewed 20 April 2022.

crime groups can use fraudulent identities to cause considerable additional (and also ongoing) financial loss.

IDCARE[27] assists thousands of Australians impacted by scam calls and SMS each year. Telephone scams represented 15% of all its client engagements in 2019, and had risen to 27% by 2021.[28] In the 3-year period from 2019 to 2021, IDCARE stated:

> '(We) provided help and support to over 10,000 Australians who had not only engaged with telephone and SMS scammers but had also experienced other crimes being committed in their name as a result of the scam engagement, such as unauthorised account access and new account establishment across industry and government. This underpins the nature of this crime and the permeations felt by victims well after the initial call or text message across industries and sectors and not just within the confines of the telecommunications industry.'[29]

Australians who are the victim of identity theft typically suffer both financial loss and psychological harm. The consequences can include experiencing reputational damage and health problems to mental and emotional distress. The effects can be life-altering: impacting health, emotional wellbeing and relationships with others.[30]

Once a customer has had their identity stolen, it can be very difficult and time-consuming to reverse the effects. IDCARE found that its clients took, on average, 33.7 days to detect the compromise of their personal information. In comparison, it took only an average of 6.9 days from the initial theft of personal and account information for criminals to commit multiple identity crimes with that information.[31]

AIC also found that victims required 34 hours on average to deal with the consequences of their personal information being misused[32] while IDCARE estimated that an average of 32 hours is spent by customers to address identity theft.[33] These figures do not include lost productivity, where a customer has taken time off work to address identity theft.[34]

Identity theft has long-term repercussions as victims can also experience multiple instances of fraud over months or years. IDCARE recommends victims to set up yearly reporting to allow for continual monitoring.[35]

Reported scams and losses

The true impact of scams on Australians remains unknown as reports and losses are almost certainly under-reported because many scam victims are embarrassed by being scammed. Victims may report their experiences in many ways – from discussing

[27] IDCARE launched in 2014 as a unique joint-public-private not for-profit national support body for victims of identity crimes, scams, and cybercrimes.
[28] IDCARE 2022, IDCARE submission to the CA consultation on *Reducing scam calls and scam SMS code*, viewed 7 April 2022.
[29] ibid.
[30] Identity Theft Resource Centre, 2018, *The aftermath – the non-economic impacts of identity theft*, viewed 14 April 2022.
[31] IDCARE unpublished data supplied to Australian Institute of Criminology for *Identity crime and misuse in Australia*, 2019, viewed 12 April 2022.
[32] Australian Institute of Criminology, 2020, *Identity crime and misuse in Australia 2019*, viewed 12 April 2022.
[33] IDCARE 2018, 'Unauthorised Mobile Phone Porting Events', IDCARE Insights bulletin.
[34] ibid.
[35] Australian Institute of Criminology, 2019, *Identity crime and misuse in Australia*, viewed 29 March 2022.

what occurred with family and friends, through to complaining to consumer advocacy organisations, notifying their financial institution or making an official report to police.

Scamwatch is the primary government website used by Australians to report scams. However, it is estimated only around 13% of all victims of scams will make a report to Scamwatch.[36]

Victims may also report to one or all the government or consumer agencies that take reports, such as the ACCC's Scamwatch, the ACMA, Telecommunications Industry Ombudsman (TIO), IDCARE[37] or the ACSC.[38] Or victims can be so overwhelmed by the available options that they decide to do nothing and exit the painful experience without reporting at all.[39]

ACMA research into the consumer experience of unsolicited communications in Australia also found underreporting is a major issue.[40] In the 6 months leading up to the 2021 survey, 98% of Australians had received some form of unsolicited communication:

- 86% of Australians received at least one scam call; 40% at least once a week
- 51% of Australians received at least one scam text; 9% at least once a week
- between 74% and 86% of Australians are annoyed by scam calls; and around 33% feel anxious, distressed or vulnerable
- Yet only 15% of call recipients made a complaint, and for texts it was only 7%.[41]

Around 33% of people who had lost money to scams did not report that loss to any organisation – resulting in financial losses to scams being grossly understated.[42]

For some victims, reporting also can be made more difficult by virtue of their background, age, language skills or disability. In 2020, ACCC's Scamwatch reported people who identified as culturally and linguistically diverse (CALD) Australians represented 5.45% of all reports made to Scamwatch (over 11,700), but 12.6 % of all losses (over $22.1 million).[43] This represents a 50% increase in reports from 2019 as well as an increase of 61% in losses. Some members of CALD communities suffered higher losses on average than the overall community, accounting for $1 in every $8 lost.[44]

First Nation Australians made up 1.6% of all reports to Scamwatch (over 3,400) and 1.1% of total losses (over $2 million) in 2020. While more than 3,400 scams were reported, fewer than 600 experienced a financial loss. However, 35.7% involved a loss of personal information in 2020, compared to 25% from non-Indigenous victims.[45]

In 2020, people with disability made 3.5% of all reports to Scamwatch and comprised 5.5% of total losses (7,500 reports to Scamwatch with $9.7 million lost) – and a third of

[36] ACCC 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 29 March 2022.
[37] IDCARE is Australia and New Zealand's national identity and cyber support service. It was formed to address a critical support gap for individuals confronting identity and cyber security concerns.
[38] ACCC 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 29 March 2022.
[39] Australian Institute of Criminology, 2019, *Identity crime and misuse in Australia*, viewed 29 March 2022.
[40] ACMA 2021, *Unsolicited communications in Australia: Consumer experience research 2021*, viewed 3 May 2022.
[41] Ibid.
[42] ACCC 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 29 March 2022.
[43] ACCC 2021, *Targeting scams: report of the ACCC on scam activity 2020*, viewed 14 June 2022.
[44] ibid.
[45] ibid.

all such reporters lost personal information to a scammer – higher than the 25% experienced by people without disability.[46]

Our consumer research indicates that older Australians are less likely to take action to manage unsolicited texts, including scams, than younger demographics. For example, only 23% of those aged 55 and over checked an unsolicited text contact by using a look-up service, as opposed to 38% of those aged 18–54. Meanwhile, 80% of those aged 55 and over reported using blocking on their phone, compared to 85% of those aged 18 to 54. This strongly suggests that older Australians are more vulnerable to receiving scam SMS.[47]

Scamwatch reports of scams 2021[48]

Contact channel	Total monetary loss	Number of scams reported	Reports with financial loss (F/L)	Average loss scam	Average loss of reports F/L
SMS	$10,100,000	67,180	8.9%	$150	$1,700
All channels	$323,723,000	286,602	8.9%	$1,130	$13,000

Data from Scamwatch indicates that in 2021 there were over 286,600 reports of scams and over $323.7 million in losses. About 23% of all Scamwatch reports were attributable to SMS (67,180 reports). These reports generated more than $10 million in losses – 3 times the losses reported in 2020 ($3.1 million). This equates to an average loss of $150 per reported SMS scam in 2021.[49]

The volume of scams reported as being delivered by SMS continues to grow considerably year on year. In 2021, there was a 107% increase in reports from 2020 (32,337) – which was already up 16% compared to 2019 (27,894 reports).[50]

Early indications are showing the rise in scams continues. From January to March 2022, Scamwatch reported that financial losses associated from SMS scams increased by a staggering 331% for the same period the previous year (approximately $1 million to over $4 million).[51]

In the same period, scam call complaints to Scamwatch and the ACMA have dropped dramatically – a 49% decrease for Scamwatch and 70% decrease for the ACMA. This suggests that the RSC code (which places regulatory obligations on providers to block calls from scammers) is having an impact.[52]

[46] ibid.
[47] ACMA 2021, *Unsolicited communications in Australia: Consumer experience research 2021*, viewed 3 May 2022.
[48] ACCC 2022, *Scamwatch scam statistics*, viewed 20 April 2022.
[49] ACCC 2021, *Types of scams: flubot*, viewed 6 April 2022.
[50] ACCC 2022, *Scamwatch statistics*, viewed 6 April 2022.
[51] Ibid.
[52] ACMA 2022, Internal complaints data; ACCC 2022, *Scamwatch statistics*, viewed 10 June 2022; ACCC media release 2022, *Australians are losing more money to investment scams*, viewed 15 June 2022.

International experience

Fuelled by ever-increasing globalisation and digitalisation, scammers can commit financial crime with increasing efficiency and sophistication. This undermines global financial systems, impedes economic growth and causes huge losses to businesses and individuals worldwide. International telecommunications regulators are responding to the challenge of combating scammers but so far, there is no single or simple solution to preventing scams delivered by SMS.

UK

In 2018, mobile providers through Mobile UK and the Mobile Ecosystem Forum (MEF), supported by the UK regulator Ofcom, launched 'SMS PhishGuard'. This initiative developed a SenderID Protection Registry involving the banking industry and government agencies where participants could register and protect the message headers used when sending texts to consumers.

The registry reduces the ability for scammers to send texts impersonating a brand in the message header by providing a check on whether the sender using that sender ID is the registered party. MEF reported in 2021 that there are now more than 70 bank and government brands being protected by the registry, with over 1,500 unauthorised variants being blocked, including 300 sender IDs relating to the UK Government's coronavirus campaign.[53]

While these solutions have had some positive results, the problem of scam calls and texts continues to evolve, requiring new and updated solutions from Ofcom, the telecoms industry, and a number of other organisations. In a recent survey, Ofcom found that more than 8 in 10 (82%) of UK adults said they had received a suspicious message, in the form of either a text, recorded message or live voice call to a landline or mobile, over the previous 3 months. This represents an estimated 44.6 million adults in the UK. Texts are the most common form of suspicious message, with 7 in 10 people (71% of respondents) reporting that they had received suspicious texts.[54]

In February 2022, Ofcom outlined its role and approach to tackling scam calls and texts. It seeks to strengthen its rules and guidance on what providers should do to make it harder for scammers to use communications services to reach consumers.[55] Ofcom's proposed initiatives include strengthening rules and guidance for providers to detect and block 'spoofed' numbers, developing a good practice guide to help prevent scammers accessing valid phone numbers and updating the do-not-originate scheme to protect legitimate numbers that are most likely to be spoofed by scammers.

USA

In 2021, the US Federal Communications Commission (FCC) that regulates telecommunications providers received nearly 378,000 reports of fraud originating via text message, resulting in US$131 million in losses – with a median loss of US$900 per fraud incident.[56] These figures were up on 2020, which saw US$86 million reported lost from nearly 335,000 reports – a median loss of US$800.[57]

As of 31 March 2022, the FCC had received over 73,000 reports of fraud originating via text message with US$64 million in losses for an average median loss of US$1000.[58] Of those reports, 6% had a dollar loss reported. In the same period in 2021, 4% of reports of fraud originating via text had a loss reported – from nearly

[53] MEF 2022, *SMS SenderID Protection Registry*, viewed 20 April 2022.
[54] Ofcom 2021, *Scams Survey*, viewed 20 April 2022.
[55] Ofcom 2022, *Tackling scam calls and texts*, viewed 20 April 2022.
[56] Federal Trade Commission (FTC) 2022, *Fraud Reports | Tableau Public*, viewed 20 April 2022.
[57] ibid.
[58] Federal Trade Commission (FTC) 2022, *Fraud Reports | Tableau Public*, viewed 20 April 2022.

94,000 reports with US$20 million lost – for a median loss of US$800. This suggests the 2021 total will be surpassed this year.

In April 2022, the Federal Communications Commission (FCC) announced that combatting unlawful robocalls and malicious caller ID spoofing was a top consumer protection priority.[59]

NZ

In NZ, the Department of Internal Affairs (DIA), the Telecommunications Forum, CERT NZ (NZ Government cyber security organisation) and the mobile network providers Vodafone, Spark, 2Degrees and Vocus work together to encourage the public to be on the lookout for harmful scam messages.

They work together to try to block web addresses used in attacks from scammers.[60] Telcos look to track down the URL host and get them to take it down. This can happen immediately, but generally takes several days depending on 'how helpful the hosts want to be'.[61] Telcos can also work with international partners to block the sites as they pop up, or block numbers that are sending out the text messages. This works fine in theory, but in practice the scammers will use fake numbers or real numbers that are owned and used by real people who have been infected by the malware.

Online scams and spam (unwanted commercial email, fax, SMS and other instant messages) can be reported to CERT NZ, NZ Police, the DIA, Netsafe or individual telecommunication agencies who all share the responsibility of dealing with the harm. In 2021, nearly 9,000 incidents were reported to CERT NZ, a 13% increase on 2020. Individuals, small businesses and large organisations from all over New Zealand submitted incident reports. Scams and fraud accounted for almost NZ$11.9 million (71%) of the total financial loss reported in 2021.[62] DIA has also established a reporting system for text scams and advises consumers to report via '7726' (SPAM).

Canada

The Canadian Anti-Fraud Centre (CAFC) reported that 2021 was a record year for financial losses, with over CA$379 million reported lost to scams and fraud in 2021. CAFC reports this was an increase of 130% compared to 2020. The CAFC also estimates that only 5% of all fraud cases are reported, so the true impacts are expected to be significantly higher.[63]

The CAFC and the Royal Canadian Mounted Police's National Cybercrime Coordination Unit are working together to develop a new national reporting system for individuals, businesses, and other organisations to report fraud and cybercrime incidents to law enforcement. The new system is expected to officially launch in Canada in 2023–24.[64]

[59] ibid.
[60] TCF 2022, *Huge surge in scam messages*, viewed 5 May 2022.
[61] ibid.
[62] CERT NZ 2022, Quarterly report summary 2021, viewed 5 May 2022.
[63] Royal Canadian Mounted Police 2022, Fraud Prevention Month raises awareness after a historic year for reported losses, viewed 4 May 2022.
[64] ibid.

Why is government action needed?

As outlined in this document and in the RISC RIS, Australians rely on telecommunications networks to access information and essential services. In the past decade, developments in digital products and services have reshaped business models, global markets, consumer experience and expectations. Major services such as social media, email providers and government agencies now use mobile phones for password resets and multi-factor identification purposes. There is increasing interest in stealing phone numbers because banks often send multi-factor identity verification or authentication codes over SMS.

These emerging technologies have also resulted in a greater consumer expectation that access to those services is appropriately safeguarded from harms. The potential for scammers to circumvent individual mobile C/CSP-level initiatives (including by moving activity to another CSP) means there is a need for government to act now to encourage industry-wide solutions to be adopted.

Scammers are relentless, and the problem of scams delivered by SMS continues to grow year on year – despite concerted efforts by government, law enforcement and industry to limit scams perpetrated on telecommunications networks. It could be considered a market failure, as the scale and impact of SMS scams continue to impose a negative externality on consumers.

Malicious SMS has generally been an end-user or application-level problem. That is, a problem for individual customers and software developers, but not – with limited exceptions – for telecommunications providers. In the last few years, mounting public and government pressure has led to providers trying to address the problem.[65] Yet, the disparate and individual approaches taken by mobile C/CSPs have not reduced the impact of scams being delivered by SMS.

This is a fight that requires a concerted, ongoing, cooperative and adaptive response from governments working with industry to strengthen the framework to protect consumers. Government action is required to address the evolving and growing consumer detriment from scams – particularly as uncertainty and disruption caused by events like COVID-19 creates more potential for consumer harm and opportunities for identity crime and fraud. Any gap in efforts to prevent scams by not collectively addressing scams delivered by SMS will likely be ruthlessly exploited by scammers, as evidenced directly by complaint and loss data in relation to SMS scams.

Strengthening the system

The objective is to strengthen the frameworks to protect consumers and reduce the incidence of fraud and identity crime from scams occurring, given the realised harms and potential for Australians to experience significant impacts.[66] We seek a measurable reduction in the prevalence of scams delivered by SMS on Australian telecommunication networks, and reduced financial and other harms to consumers.

[65] ABC News 2022, *Telstra rolls out SMS scam filter in response to surge in dodgy mobile phone texts*, viewed 22 April 2022.

[66] Former Minister for Communications, Cyber Safety and the Arts, Paul Fletcher MP media releases, 2020 and 2021, *New Standard to fight fraudulent number porting*, *Stopping ATO phone call scams*, *Detecting tracing and blocking scam calls*, *Protecting Australians from scam texts*, viewed 20 April 2022.

However, international and local experience indicates that there is no single nor simple solution to preventing fraud and reducing scams perpetrated over telecommunications networks. Technological solutions to scam disruption need to sit within a broader framework to be effective. Accordingly, in 2018, we established the cross-agency Scam Technology Project with the ACCC and the ACSC – with inputs from industry – to explore ways to reduce scam activity over telecommunications networks.[67]

Australian governments want to work with regulators, law enforcement agencies and industry to keep Australians safe from harm. In November 2019, the ACMA's 3-point *Combating scams action plan* was released. The recommendations actioned included forming a joint government-industry taskforce (STAT),[68] immediately trialling new scam reduction initiatives and developing new enforceable obligations. Actions for the enforceable obligations recommendation included implementing and updating SMS filtering technology, providing advice and information to customers, and monitoring broader technological development and international initiatives for potential implementation.

The Australian Cyber Security Strategy 2020 sets out the government commitment to support the telecommunications industry to implement threat blocking technology to prevent the proliferation of scams over the telecommunications network and protect the public from malicious scams. Industry has also trialled initiatives such as piloting a program with government agencies to identify and reject illegitimate phishing text messages impersonating myGov and Centrelink[69] and, in some cases, rolling out a SMS scam filter to improve monitoring and blocking of suspected scam SMS.[70]

In 2021, the Department of Home Affairs made the Telecommunications (Interception and Access) Amendment (2021 Measures No. 1) Regulations 2021. It sets out the matters that a court may have regard to when considering if exceptions apply to the general prohibitions on intercepting telecommunications contained in the *Telecommunications (Interception and Access) Act 1979*. This effectively provides comfort for C/CSPs to intercept malicious text messages and take blocking action.

As previously mentioned, in December 2020 we registered new rules requiring C/CSPs to detect, trace and block scam calls. The RSC code was the first industry code developed to specifically target the significant problem of scam phone calls.[71] The code filled a gap in the regulatory framework and remains the primary regulatory obligation for C/CSPs to prevent consumer harm from scam calls.

In the first 16 months of the RSC code being in force, more than 549 million scam calls were blocked.[72] While it is promising to see a significant reduction in scam calls, the RSC code does not address the impact and harms associated with scams delivered

[67] The ACMA Scam Technology Project explored solutions to address scam calls on Australian telecommunications networks and looked at what can be done to disrupt scam activity. *Combating scams: A discussion paper on technological solutions* was released in March 2019. Following consultation, the ACMA worked with the ACCC and the ACSC and experts from industry, government and overseas regulators to develop the 3-point *Combating scams action plan*. The plan's 3 key actions have been acquitted.

[68] The Scam Telecommunications Action Taskforce (STAT) was a key action from the *Combating scams action plan* and provides government and industry coordination and oversight of telecommunications scam minimisation strategies.

[69] Telstra, *New pilot program to block cyber criminal impersonating Services Australia*, viewed 21 April 2022.

[70] ABC News 2022, *Telstra rolls out SMS scam filter in response to surge in dodgy mobile phone texts*, viewed 22 April 2022.

[71] ACMA 2020, *RISC RIS* pp 2–4, viewed 9 June 2022.

[72] ABC News 2022, *ACCC says scam calls are increasing. Here's what you can do to avoid them*, viewed 28 March 2022.

via SMS. This gap in protections creates further opportunities for scammers which has consequences for all Australians.

In addition to the work being undertaken by governments to promote the fight against scammers and fraudsters, industry has recognised the need to develop a range of technical responses to reduce scams delivered by SMS and dovetail with proposed new obligations. It acknowledges these measures can not only reduce the associated financial loss and hardship to customers, but also build confidence in telecommunications networks.

In 2022, Communications Alliance publicly consulted on a proposed revision to strengthen the RSC code by targeting scam SMS.[73] The code revision intends to contain new provisions dealing with the identification, tracing and blocking of scam text messages, as well as continuing to provide a framework for co-operation and information-sharing among telecommunications service providers. The revised code will be supported by an updated confidential industry guidance note which provides detailed operational information to support C/CSPs to comply with the code's additional obligations. The guidance note will not be publicly available due to concerns about how it may be used by scammers.

The potential for scam traffic to circumvent individual provider level blocks means government action that requires the telecommunications industry to take collective action to strengthen processes to prevent scams delivered by SMS provides the strongest incentive to achieving the best outcome for the Australian community.

[73] ACMA media release 2022, *Scam crackdown results: Telcos block half a billion scam calls*, viewed 3 May 2022.

What policy options have been considered?

The Telecommunications Act sets out the regulatory policy that the Parliament intends the telecommunications be regulated in a manner that 'promotes the greatest practicable use of industry self-regulation' and 'does not impose undue financial and administrative burdens on [industry participants]'. However, it should not compromise the effectiveness of regulation in achieving objects that include promoting the long-term interests of end-users and the availability of accessible and affordable services that enhance the welfare of Australians.[74]

The policy options considered to reduce scams delivered by SMS are consistent with the regulatory policy and objects set out in the Telecommunications Act and analysed in the RISC RIS.[75]

Option 1: Non-regulatory option (status quo)

The government encourages telecommunications providers to implement scam mitigation measures and provides general advice to consumers on avoiding scams delivered via SMS.

Under this option, mobile C/CSPs would continue with the disparate (and larger provider level) inconsistent operational approaches currently employed to reduce scam SMS activity. Consumers will experience varying levels of protection as scammers will continue to exploit and target any weak links and ineffective processes.

No compliance requirements or enforcement options would apply. Scams delivered by SMS will still reach consumers and it is likely the volume of SMS scams – and resultant harms – escalate, as no coordinated, industry-wide technological or network strategies have been deployed.

This option would not meet the objectives of the 2019 *Combating scams action plan* which recommended consistent, industry-wide robust scam verification measures and information-sharing across telecommunications providers and between providers and government (action 2).[76]

Option 2: Consumer education campaign

The government does not introduce any new form of regulation but conducts an online education campaign that builds on existing phone scam resources to provide clear and accessible information to assist consumers to better manage and avoid scams delivered by SMS. The existing legislation and regulations governing mobile C/CSPs remain.

The campaign focuses on developing resources that advise Australians how to identify scams delivered by SMS, and what to do if they receive one or become a victim. This includes support on where to report the scam and get help protecting their account or personal information.

[74] Section 4, Telecommunications Act, viewed 10 June 2022.

[75] ACMA 2020, *Reducing scam calls RIS*, p 14–16, viewed 7 April 2022.

[76] ACMA 2019, *Combating scams action plan*, viewed 15 June 2022.

The resources are promoted in collaboration with other government agencies, consumer advocacy groups and mobile C/CSPs. These activities include leveraging off existing websites and social media channels, issuing emails/letters/bulletins and establishing stakeholder and community forums.

Information is also designed for First Nations Australians, phone users who may be in vulnerable circumstances, and culturally and linguistically diverse communities to inform and help them better manage scams delivered by SMS. The resources are published online and available for general community use. However, some members of the community may still not receive nor understand the campaign information.

The campaign is run by the ACMA annually for 10 years and in accordance with usual practice builds on other phone scam resources and campaigns. A campaign based upon the steps below will cost on average around $31,000 per annum and feature:[77]

- information published on the ACMA and other government websites
- additional video tile complementing current phone scam resources aimed at providing consumers with relevant information in an accessible format
- dedicated resources with information for vulnerable communities including translations into multiple languages and designed for First Nations Australians audience
- targeted ads on social media to reach consumers (including an image, content, and link back to the ACMA website)
- use of ACMA newsletter subscriber lists and industry contacts
- boosting impressions of the social media content (potentially reaching 7.7m people).

This option relies entirely on raising consumer awareness and providing information that helps consumers to be more proactive in identifying and managing scams delivered by SMS. It supports action 2.8 in the 2019 *Combating scams action plan* to provide advice and information to customers as part of the key recommendation for enforceable obligations.

Option 3: Enforceable obligations (revised code)

Industry group Communications Alliance submits a revised 2020 RSC code for registration, providing for the ACMA to register enforceable obligations under Part 6 of the Telecommunications Act[78] to reduce the impact of scams delivered by SMS.

The revised industry code would be outcomes-focussed to allow scalable and flexible measures to block SMS to be considered to be adapted in the rapidly evolving space of cybercrime where criminals are likely to quickly try to circumnavigate them. The code introduces new requirements on mobile carriers and C/CSPs to disrupt scams delivered by SMS. It identifies measures that leverage off, and further strengthen, existing scam call prevention obligations that are in place to protect consumers.

Mobile C/CSPs would be required to:

- collaborate with other mobile C/CSPs and, where appropriate, relevant government agencies to identify, block and disrupt scams delivered by SMS (including but not limited to fraudulent SMS sender IDs) to verify that the sender is a valid subscriber and the message is coming from a valid and correct location

[77] Based on a single online consumer education campaign run annually. See Appendix A of this RIS for further details.
[78] Section 117 of the Telecommunications Act provides for industry to develop codes that are registered with the ACMA

- collaborate with aggregators and, where appropriate, relevant government agencies to identify, block and disrupt scams delivered by SMS (including but not limited to fraudulent SMS sender IDs)
- establish processes in relation to how evidence of scams delivered by SMS is gathered and shared/communicated between mobile C/CSPs, and relevant government agencies
- establish processes for mobile C/CSPs to exchange information to trace the origin of scams delivered by SMS.

As per the RISC RIS, this option provides us with powers under Part 6 of the Telecommunications Act to take action to ensure C/CSPs comply with enforceable obligations.[79] This option would support a key recommendation (action 2) in the 2019 *Combating scams action plan*[80] to develop enforceable obligations for telecommunications providers that are consistent, industry-wide robust scam verification measures (specifically actions 2.1, 2.2, 2.5, 2.6). It also supports information-sharing across telecommunications providers and between providers and government (actions 2.7 and 2.8).

[79] ACMA 2020, *Reducing scam calls RIS*, p 14–16, viewed 25 May 2022. Under Part 6 of the Telecommunications Act, the enforceable obligations options available to the ACMA are either an industry code or an industry standard. If an industry code proves deficient, then an industry standard could be considered (section 125), including under ministerial direction (subsection 125AA (4) of the Telecommunications Act).

[80] ACMA 2019, *Combating scams action plan*, viewed 15 June 2022.

What is the likely net benefit of each option?

The assessment of net benefit is informed by the following assumptions:

- costs and benefits for all options are projected forward from 2022 for 10 years
- future costs/benefits are discounted to present value using a real discount rate of 7%
- costs and benefits are reported in average annual figures.

Status quo

It can be anticipated that the impact of harms associated with scams delivered by SMS will continue to increase over time. Due to the inconsistent reporting patterns about incidents, it is likely the estimate will not capture the full scope of the problem.

Therefore, for the purposes of this RIS, an average annual increase of 25% has been applied to measure the growing consumer detriment. This considers the trend of the increasing volume of reports of scams and associated losses reported to Scamwatch concerning scams delivered by SMS.[81]

If the status quo is maintained, the Australian community (including consumers and business) will continue to be subject to scams delivered by SMS, as scammers will continue to target any Australian mobile number.[82]

Benefits

Mobile C/CSPs that have not implemented any process to monitor, verify, trace and share data on scams delivered by SMS may benefit from choosing not to implement any additional processes. However, these mobile C/CSPs may be subject to reputational loss and decreased consumer confidence.

Costs

As reported by Scamwatch, scams delivered by SMS accounted for nearly a quarter of all scam reports (67,180) and more than $10.1 million in reported losses in 2021.[83]

It can be anticipated that if the status quo remained, losses from reported scam SMS to consumers and businesses would continue to increase, and there would be on average a net cost of $179,904,000 compromising of:

- direct financial losses each year over a 10-year period of $22,420,000[84]
- indirect losses (including time and social costs) to the community of $157,483,000 each year over a 10-year period.

[81] ACCC *Scamwatch statistics 2021*, viewed 21 April 2022. This considers that the financial losses reported to Scamwatch has risen each year – from $107 million in 2018 to $323 million in 2021 (202% increase). The volume of scams reported to Scamwatch as being delivered by SMS continues to grow considerably year on year – in 2018, 14.4% of all scams were reported from SMS contact. In 2021, this had increased to 23.4% of all reported scams.

[82] ACMA 2020, *Reducing scam calls RIS*, p17, viewed 7 April 2022.

[83] ACCC *Scamwatch statistics 2021*, viewed 7 April 2022.

[84] See Appendix A Compound growth on $10.1 million over 10 years discounted at 7% each year.

Consumer education campaign

Benefits

As set out set out in the RISC RIS, it is anticipated that an online consumer education campaign will support Australians to become more informed and take measures to identify and manage scams delivered by SMS.[85]

Consumers

The practical impact of an online education campaign could result in an estimated 15% reduction in the impact of scams delivered by SMS compared to the status quo. This estimated reduction is based on similar online consumer awareness campaigns that have raised awareness and increased consumer knowledge.

Informed consumers are more likely to better protect their personal information and offer assistance to family and friends. This will help prevent harms being perpetrated – including identity theft – and reduce the significant distress, trauma and suffering that occurs due to scammers. Scamwatch hears from many scam targets who avoided becoming victims simply because they told someone about their experience, and that person recognised the characteristics of a scam and advised them that it sounded like a scam.[86]

Continuing education and awareness campaigns about SMS scams may increase reports to government as more people learn from government campaigns how to spot and stop scams delivered by SMS. Consumers will be more informed about how to protect themselves from scams delivered by SMS and know how to respond in the event of receiving one. This can be by taking greater control of how they share their personal information in public, quickly contacting their financial institution if they've been scammed, and reporting it to Scamwatch.

Informed customers may actively seek the best protection for themselves and choose a provider based on what it is doing to reduce scams delivered by SMS. This may incentivise mobile C/CSPs to voluntarily increase protections in accordance with the status quo to provide a point of difference in the market, which may also reduce instances of scams delivered by SMS.

However, information provision alone is unlikely to create widespread and long-lasting behaviour change, and the campaign would likely need to be re-run multiple times to have sustained benefit.

Mobile C/CSPs

Better informed consumers could drive more mobile C/CSPs to adopt additional protections that not only support compliance with existing obligations, but also provide reputational benefits for the provider – particularly for those mobile C/CSPs that can demonstrate their commitment to protections for their customers.

Mobile C/CSPs have obligations to do their best to prevent networks or facilities being used in commission of offences against the laws of the Commonwealth and states and territories. For example, a provider that voluntarily implements scam disruption measures by blocking suspicious SMS activity may stop thousands of consumers being targeted. Mobile C/CSPs that adopt good practices could have a competitive advantage by being able to advertise themselves as being a provider that protects consumers, contributing to the reduction in the impact of scams delivered by SMS.

[85] ACMA 2020, *Reducing scam calls RIS*, p19–20, viewed 20 April 2021.
[86] ACCC 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 20 April 2022.

Total benefit

The benefits of this option represent prevention of financial losses to scams delivered by SMS of $26,985,000[87] each year over a 10-year period comprising of:

- direct savings of $3,363,000
- savings in time spent by consumers responding to identity theft of $23,622,000[88]
- freeing up of financial institution and/or telecommunications fraud team resources by 15% each year to assist customers on other matters[89]
- a reduction in the resources required by community organisations (such as IDCARE) to assist customers who have experienced identity theft from unauthorised high-risk customer transactions (equivalent savings of 15%).[90]

Costs

As described above, the cost of the education campaign is around $31,000 per annum.

Additionally, as identified in the RISC RIS, better informed consumers may also increase workloads for both mobile C/CSPs, and financial institution fraud teams – as consumers will be more responsive to the signs of a scam.[91] While these extra costs have not been quantified but are described qualitatively, it is anticipated that financial institutions and mobile C/CSPs will continue to need to spend time and dedicate resources to respond to scams delivered by SMS. This includes detecting and analysing scams and resourcing specialist fraud teams on how to identify and address potential scams delivered by SMS.

Mobile C/CSPs may need to direct additional resources towards implementing stakeholder engagement activities or updating existing consumer information to align with online campaign activities. This includes additional time spent on training frontline staff.

Enforceable obligations (revised code)

Benefits

It is conservatively estimated that enforceable obligations will result in a 70% reduction in the impact of scams and fraud due to SMS scams.[92] This option leverages off system and process changes implemented to meet the obligations in the 2020 *Reducing Scam Calls* code as well as comply with the existing regulatory framework.

Consumers

Australian consumers can expect to benefit from the option to introduce enforceable obligations that mandates action to address scams delivered by SMS and provides increased consumer safeguards. Enforceable obligations have the potential to provide

[87] Figure based on present value of net benefits.

[88] Figure based on reduced reports of all SMS scams and time costs equivalent to $32 per hour for 33 hours, averaged and discounted over 10 years.

[89] While it is estimated that financial institutions and/or telecommunications may have reduced operating costs, this benefit has not been incorporated into the cost benefit analysis.

[90] While it is estimated that community organisations may have reduced allocation of resources, this benefit has not been incorporated into the cost benefit analysis.

[91] ACMA 2020, *Reducing scam calls RIS*, p 20, viewed 21 April 2022.

[92] Figure conservatively based on changes seen following implementation of enforceable obligations to address mobile porting fraud and scam calls (January to March 2022 – 70% reduction scam call complaints to ACMA and 49% decrease to ACCC's Scamwatch) as well as industry-initiatives to combat SMS scams.

significant positive impacts by reducing the financial and emotional harms that an individual may face from fraudulent activity.

Mandating better protections would also be consistent with the government's commitment to improve consumer safeguards and reduce instances of mobile porting fraud and scam calls. Placing enforceable obligations on mobile C/CSPs to protect consumers through blocking and disrupting SMS scams and ensuring the message is coming from a valid and correct location will also provide improved opportunities for referral for potential regulatory or law enforcement action.

The most significant benefit from enforceable obligations will be the anticipated substantial reduction in the financial and social impact on Australians.

Mobile C/CSPs

Regulations combating scams delivered by SMS would only apply to mobile C/CSPs. Enforceable obligations (via a revised code) provide the opportunity to encourage consistent, industry-wide approaches to combating scams delivered by SMS by establishing processes and protections that provide certainty for mobile C/CSPs and their customers.[93] With all mobile C/CSPs treated the same, there is a competition benefit as providers can promote themselves as having responsive fraud detection and customer protection services in place.

Indirectly, mobile C/CSPs and financial institutions will benefit from spending less time and resources responding to complaints about scams delivered by SMS, as well as assisting consumers to manage the impact. Additional action by mobile C/CSPs to act against scams delivered by SMS and share information about scams delivered by SMS with other providers will become more effective as the market is covered by protections. If all providers are working cooperatively to address scams delivered by SMS, the Australian telecommunications ecosystem is better protected.

A collaborative approach to addressing scams delivered by SMS provides a reputational benefit for mobile C/CSPs. It demonstrates to consumers that they are taking concerted, industry-wide steps to improve consumer safeguards and disrupt scams delivered by SMS. Collaborating to reduce scams delivered by SMS provides positive benefits for providers when their networks and services are more safe and secure. This benefit accrues from consumers who are satisfied with extra protections, as well as businesses who appreciate the secondary protections afforded to their customers through enforceable obligations.

In addition, mobile C/CSPs – who are relentlessly targeted by scammers impersonating their brands and attempting to steal the identity of their customers – benefit from the extra protections.

Total benefit

Initial benefits of this reduction represent prevention of financial losses to scams delivered by SMS of $125,932,000[94] each year over a 10-year period comprising of:

- direct savings of $15,694,000
- savings in time spent by Australians responding to identity theft of $110,238,000[95]

[93] ACMA 2020, *Reducing scam calls RIS*, p 21–22, viewed 19 April 2022.

[94] Figure based on bet benefits net present value.

[95] Figure based on reduced reports of all SMS scams at a rate of $32/hour for 33 hours, averaged and discounted over 10 years.

- freeing up of financial institution and/or telecommunications fraud team[96] resources by estimated equivalent 70% each year to assist customers on other matters
- a reduction in the resources required by community organisations (such as IDCARE) to assist customers who have experienced identity theft from unauthorised high-risk customer transactions (equivalent savings of 70%).[97]

Costs

Consumers

There are no direct costs to consumers from enforceable obligations (revised code).

Mobile C/CSPs

For the purposes of this RIS, the number of mobile C/CSPs which will be covered by enforceable obligations has been conservatively estimated at a maximum of 178 – including an estimated 20 SMS aggregators. This estimate includes each mobile C/CSP, however there are several partnerships and carrier relationships in place. For example, some smaller mobile CSPs are owned by larger C/CSPs while others purchase network capacity to provide services to their customers.

Mobile C/CSPs have been characterised as follows (based on the volume of mobile service numbers allocated by the ACMA):

- large mobile C/CSPs: 3 (over one million)
- medium mobile CSPs: 26 (100,000 to one million)[98]
- Small mobile CSPs: 19 (10,000 to 99,999)
- Very small mobile CSPs: 130 (less than 10,000).

Providing for enforceable obligations that are technology-agnostic and outcomes-focussed will provide flexibility for mobile C/CSPs to determine how they will monitor its network to detect and act against scams delivered by SMS. For example, it may be more efficient for mobile C/CSPs to automate their systems to comply with obligations, but for a small mobile CSP with fewer customers, it may be more efficient to conduct the necessary activities manually.

In addition, mobile C/CSPs have invested in complying with the RSC industry code for administrative processes or network strategies to strengthen procedures and block high-volume call traffic that can be leveraged to capture high-volume SMS traffic on mobile networks.

Where costs accrue under enforceable obligations, feedback provided by industry members as they developed the obligations indicated that costs will be higher for carriers due to their role in the telecommunications ecosystem. This is because they provide the basic transmission infrastructure on which carriage and content services are supplied to the public. Carriers operate international gateways carrying internationally originating traffic (including scams delivered by SMS) onto domestic networks, and working with international carriers to reduce scams delivered by SMS should lessen the burden across the rest of the Australian telecommunications industry.

[96] While it is estimated that financial institutions and/or telecommunications may have reduced operating costs, this benefit has not been incorporated into the cost-benefit analysis.

[97] While it is estimated that community organisations may have reduced allocation of resources, this benefit has not been incorporated into the cost-benefit analysis.

[98] Six mobile providers qualified as medium MCSPs. The ACMA does not receive aggregator data but has assumed an additional 20 MCSPs in the form of aggregators may incur similar costs to a medium-sized MCSP. This will be dependent on the substance of regulations introduced.

As Table 1 below shows, given the work undertaken in year 1, it is assumed the processes will improve with staff being more experienced and technology improved, and that the volume of scams delivered by SMS requiring blocking action decreases. Costs to comply with the obligations would drop significantly from year 2 and mainly reflect the activity involved in sharing information with other mobile C/CSPs.

Table 1: Costs to all mobile C/CSPs to comply with enforceable obligations over 10 years[99]

Category	Costs year 1	Cost year 2 onwards
Large	$3,015,000	$614,000
Medium	$5,330,000	$1,160,000
Small	$343,000	$108,000
Very small	$1,047,000	$478,000
Sub-total	$9,734,000	$2,360,000
Less 70% year 1	$6,814,000	
Total	**$2,920,000**	**$2,360,000**

Regulatory burden measurement

The regulatory burden measurement (RBM) is calculated consistent with government guidance[100] and provided as a simple average of costs to industry over the first 10-year period (2023–32) using 2022 values. Costs have been disaggregated by the following cost types:

- administrative compliance costs – costs that are primarily driven by the need to demonstrate compliance with the convention (such as annual reporting)
- substantive compliance costs – that are directly attributable to the reform option and fall outside of the usual business costs. These costs may include the capital costs as well as operational costs from process changes or additional staff training
- delay costs were considered but do not apply in relation to the options considered in this RIS.

See table 2 below for the total industry average industry costs over the 10-year period.

[99] Estimated costs are expressed in 2022 dollar terms. For further detail on breakdown of costs, see Appendix A.

[100] Office of Best Practice Regulation 2021, Regulatory Burden Measurement Framework, viewed 18 May 2022.

Table 2: Regulation burden measurement

Option	Regulatory cost (annual)
Status quo	n/a
Consumer education campaign	n/a
Enforceable obligations (revised code)	$2,416,000

The RBM focuses on the costs to industry that would not otherwise be incurred. Business-as-usual costs (being those arising from existing legislation or actions that industry would undertake regardless of government intervention), are excluded from the calculation.

Likely annual benefit over 10 years

Factoring in the regulatory burden measurement, we anticipate that the option that will provide the best net benefit for the Australian community is Option 3: Enforceable obligations (revised code).[101]

[101] See Appendix B for further detail on options.

Table 3: Summary results (in present value terms)

Options[102]		Status quo	Education campaign	Enforceable obligations (revised code)
Effectiveness of intervention: % reduction in scams delivered by SMS		0	0.15	0.7
Cost	Costs to customers (direct)	-$22,420,425		
Cost	Costs to customers (time)	-$157,482,658		
Cost	Cost of education campaign		-$31,188	
Cost	Regulatory costs			-$1,829,423
Benefit	Reduced scams delivered by SMS to customers		$3,363,064	$15,694,297
Benefit	Reduced customer time costs		$23,622,399	$110,237,860
Total status quo cost		-$179,903,082		
Total incremental cost		-	-$31,188	-$1,829,423
Total incremental benefit		-	$26,985,462	$125,932,158
Net incremental benefit (or net benefit)		-	$26,954,274	$124,102,735
Benefit to cost ratio (BCR)		-	865	69

The central case provides a net benefit and the project provides a return of $69 for every $1 invested. Note that the word 'incremental' is used where the cost or benefits are incremental to the status quo situation.

[102] Assumes 25% annual growth in scams delivered by SMS, and a discount rate of 7%. This table has factored in regulatory costs as detailed in the regulatory burden measurement table, which is based on a conservative overestimation of the number of mobile C/CSPs which will incur regulatory costs.

Who was consulted and what did they say?

As previously discussed in the RISC RIS, significant stakeholder engagement and consultation has occurred around measures to reduce the impact of scam calls.[103]

A working group drawn from the government members on the Scam Telecommunications Action Taskforce (STAT) – and chaired by the ACSC – was established in July 2020. Its goal was to explore solutions to reduce scams delivered by SMS – particularly government and trusted brand impersonation scams. The working group comprised government agencies (including the Australian Taxation Office, Australia Post and Services Australia), and technical, fraud and regulatory officers from industry (including Pivotel, Telstra and Sinch). The ACMA participated as an observer on the working group which initially convened to consider whether international initiatives (specifically, the UK's Sender ID registry[104]) could be deployed in the Australian communications environment.

Working group members identified the need to extend consideration of solutions more broadly and not limit their consideration to a specific solution. The working group reformed as the SMS Phishing Protection Working Group sharing information and intelligence to disrupt scams delivered by SMS.

In November 2020, the Communications Alliance working committee that developed the registered RSC code commenced considering initiatives to reduce scams delivered by SMS. It represented the first major industry-wide action to tackle scams delivered by SMS. The committee includes key mobile C/CSPs and aggregators, and has been focused on developing consistent industry processes to disrupt scams delivered by SMS. This has included a review of the RSC code to identify measures that can leverage off existing systems and processes and replicate the effectiveness of the voice call scam mitigation rules contained in that code.

In late 2021, STAT working group members agreed that Communications Alliance was best placed initially to consider how existing obligations to detect, trace and block phone scams could be applied to scams delivered by SMS to broaden consumer safeguards and ensure scammers' efforts were not redirected.

The ACMA participates as an observer on the Communications Alliance Working committee to identify and build on initiatives to combat phone scams. Both the STAT working group and CA working committee support practical measures to disrupt scams delivered by SMS by revising the RSC code.

On 9 February 2022, Communications Alliance commenced public consultation on a draft *Reducing Scam Calls and Scam SMs (short messages)* industry code. The consultation closed on 11 March 2022. Communications Alliance received 24 submissions from individuals, government (including the ACMA) and law enforcement agencies, telecommunications providers and organisations representing the interests of consumers.[105]

---

[103] ACMA 2020, *Reducing scam calls RIS*, p 27–28, viewed 28 April 2022.

[104] Mobile Ecosystem Forum, 2018, *SMS Sender ID Protection Registry*, viewed on 5 May 2022.

[105] Communications Alliance 2022, Public submissions – Comment sought on Revised C661:2022 Reducing Scam Calls and Scam SMs Industry Code, viewed 5 May 2022.

Submissions unanimously welcomed a review of the code and overwhelmingly supported the addition of new rules for industry to reduce the harms from scams delivered by SMS. The key matter raised in stakeholder submissions related to the use of numbers, i.e., whether a CSP needed to 'hold'[106] a number to provide a service to a customer in association with the number. This issue is associated with, but not directly relevant to action to prevent scams. While submissions from individual CSPs were split on this issue, the Communications Alliance working committee[107] subsequently reached a consensus position in drafting the revised code that requires 'originating' CSPs to prevent carriage of a call where the A-Party (or 'initiating' CSP) does not hold the Rights of Use to the number.[108] This revised drafting resolved the matter and was endorsed by the working committee.

ACCAN and the Australian Federal Police (AFP) were both concerned with timeframes and the ambiguity of language. The AFP provisions relied on the effectiveness of internal monitoring processes and recommended C/CSPs have documented processes. AFP also suggested timeframes for compliance be included within the code.

ACCAN raised the issue that ambiguous language may lead to unnecessary delays in unblocking public numbers. These delays would leave consumers without service longer than necessary as where a public number is found to be incorrectly blocked, a C/CSP must take action to unblock that public number 'as soon as practicable'. ACCAN suggested consumers would benefit from an explicit time window to reduce unnecessary disruption of their service and suggested a time window of 24 hours to unblock an incorrectly blocked public number.

In response to this feedback, the working committee incorporated a new section formalising the reporting of scam calls and SMS to the ACMA. It decided timeframes for processes would remain in the confidential industry guideline to prevent scammers gaining access to information; however, a clause was added to the industry code stating that the guideline must be adhered to by industry participants.

Communications Alliance is also required to consult with the ACCC, the Office of the Australian Information Commissioner (OAIC), the TIO and at least one body or association that represents the interests of consumers has been consulted about the development of the code (ACCAN). Communications Alliance has provided evidence to the ACMA to substantiate that appropriate consultation was undertaken with the ACCC, OAIC and the TIO.

As per section 117 of the Telecommunications Act, once the code is submitted for registration, the ACMA must also consult with the OAIC that it is satisfied with such a code – particularly if it deals with matters under the Privacy Act. The ACMA consulted OAIC and received confirmation it was satisfied with the code. We are satisfied that Communications Alliance met its consultation requirements as per section 117 of the Act.

[106] Under the Telecommunications Numbering Plan 2015, a CSP 'holds' a number if it has been allocated or transferred to it and the number has not subsequently been transferred to another CSP, surrendered or withdrawn.

[107] Working committee members are drawn from telecommunications industry participants including the Australian Mobile Telecommunications Association (AMTA), Optus, Pivotel, Sinch, Symbio, Telstra, TPG Telecom, Twilio, Verizon and Vocus.

[108] Right of Use has the meaning given by industry code *(C566:2005) Rights of Use of Numbers* or such other registered industry code that replaces (*C566:2005) Rights of Use of Numbers*.

What is the best option from those considered?

Enforceable obligations

Preventing scams presents serious challenges to industry and government as scammers are technologically adept, sophisticated and show no signs of stopping. Australians are at risk from the impact of considerable harms. This emphasises the need for government to enforce practical technological solutions that increase the effectiveness of preventing and disrupting scam activity on Australian telecommunications networks.

Consultation and engagement to date indicates that enforceable obligations (through revising the existing RSC code) are supported by C/CSPs, individuals, government and community organisations. Although the education option (Option 2) has the highest benefit to cost ratio, the highest net benefit in present value dollar terms is the enforceable obligation option (Option 3). For that reason, Option 3 is the preferred option.

A revised code allows industry expertise regarding technical capacity and also allows for the code to be reviewed to incorporate continuous improvement practices as network capability improves. Extending the enforceable obligations in the existing code to SMS provides more robust protections for customers through introduction of measures requiring SMS scam disruption. These protections do not impose undue financial and administrative burdens on mobile C/CSPs and significantly improve protections for the Australian community. Considering the telecommunications industry has already absorbed costs to implement processes and systems to meet its obligations under the existing industry code, extending these obligations to scams delivered by SMS will not cause unreasonable nor undue financial cost and administrative burden.

Status quo

The status quo (Option 1) has large costs to consumers and businesses, posing an unacceptable level of customer harm, including from direct and indirect costs associated scams delivered via SMS.

The community will continue to experience increasing levels of harm because of scams delivered via SMS as no consistent, coordinated, industry-wide technological or network strategies have been deployed. The impact of harms, including from ongoing psychological distress and the potential for repeated instances of identity theft and fraud, remains.

Consumer education campaign

The education campaign (Option 2) may provide some benefits to the community to support a reduction in financial losses and ongoing psychological distress. This includes providing information that encourages Australians to identify and manage scams delivered via SMS and increasing awareness and options to protect digital identities. However, it does not match the significant benefits of placing enforceable obligations on mobile C/CSPs to ensure consistent practices to reduce the impact of scams delivered via SMS. Additionally, we note that the enforceable obligations approach will support a level of consumer awareness-raising that also supports consistent, industry-wide practices.

How will you implement and evaluate your chosen option?

Communications Alliance submitted its revised industry code – *Reducing Scam Calls and Scam SMs* – to the ACMA incorporating new obligations on mobile C/CSPs to reduce the impact of scams delivered by SMS. Where we are satisfied the code meets section 119A of the Telecommunications Act requirements, we must approve the code – consequently registering a new code. It is not a delegated decision.

In order to meet the objective of reducing the impact of scams delivered by SMS, the enforceable obligations will be evaluated as part of our monitoring and compliance activities. SMS scams will be a compliance priority for the ACMA in 2022–23.[109]

As referenced earlier, obligations to reduce the impact of scams delivered by SMS will apply only to mobile C/CSPs. While some individual providers have led the way for the rest of industry, implementation of the new measures may be challenging, particularly for smaller mobile CSPs. We will engage with Communications Alliance and the AMTA to support industry-led awareness raising activities about the new obligations. This may include by providing additional guidance leading up to and following the introduction of the code, and encouraging industry to develop enhanced technical and operational capacity to detect and block scams delivered by SMS.

The ACMA will monitor the implementation of enforceable obligations and evaluate measures through built-in review points with the code scheduled to be reviewed within 2 years of registration. The code will also be reviewed every 5 years, or earlier in the event of significant developments that affect it or a chapter within the code.

We will receive quarterly reports from industry on the number of blocked SMS. The ACMA will also monitor our complaints and those received by the ACCC's Scamwatch and the TIO – including complaints about industry practice to comply with the code and the number of scams delivered by SMS.

We will leverage off our stakeholder networks (including under STAT) to engage with other interested stakeholders and look for opportunities to leverage off scam mitigation activities across government and industry. We have Memorandums of Understanding in place with the US, Canadian and New Zealand regulators and are actively engaged with our fellow regulators in the UK and Singapore to share information and intelligence about scam reduction initiatives.

We will actively enforce compliance with the new enforceable obligations in line with the legislative framework (as discussed in the background section of this RIS). Civil penalties could be pursued through the Federal Court or an infringement notice issued if a direction to comply is then breached (under Part 31 of the Act). If an industry code proves deficient, then an industry standard could be considered (section 125), including under ministerial direction (subsection 125AA (4) of the Telecommunications Act).[110]

[109] ACMA 2022, ACMA compliance priorities 2022–23, viewed 27 June 2022.
[110] *Telecommunications Act 1997*, viewed 9 June 2022.

The ACMA exercises these powers using a graduated and strategic risk-based approach to compliance and enforcement action. It will be important to revisit existing interventions to check whether they remain fit-for-purpose in the current environment and how protections can be assured in the future. Should the measures prove ineffective and not meet the objective of reducing the harm from scams delivered by SMS, we may consider regulatory reform or advice to government about implementing new rules more suitable to addressing harms and any regulatory gaps.

Appendix A: Calculations to inform the regulatory burden measurement

Year One	System build	Time (hours)	Businesses	Rate/hour ($)	Totals ($)	Year Two	System upgrade	Time (hours)	Businesses	Rate/hour ($)	Totals ($)
Large carriers						**Large carriers**					
Automate manual systems to monitor and block for scam SMS	$ 1,000,000		3		$ 3,000,000	Monitor and block scam SMS	$ 200,000		3		$ 600,000
Automate processes to share information meet obligations		52	3	$ 74	$ 11,603	Share information to verify and block		52	3	$ 74	$ 11,603
Staff training		15	3	$ 74	$ 3,347	Staff training		10	3	$ 74	$ 2,231
TOTAL					**$ 3,014,950**	**TOTAL**					**$ 613,835**
Medium carriers/CSPs						**Medium carriers/CSPs**					
Automate manual systems to monitor and block for scam SMS	$ 200,000		26		$ 5,200,000	Monitor and block scam SMS	$ 40,000		26		$ 1,040,000
Automate processes to share information		52	26	$ 74	$ 100,562	Share information to verify and block		52	26	$ 74	$ 100,562
Staff training		15	26	$ 74	$ 29,008	Staff training		10	26	$ 74	$ 19,339
TOTAL					**$ 5,329,570**	**TOTAL**					**$ 1,159,901**
Small CSPs						**Small CSPs**					
Automate manual systems to monitor and block for scam SMS	$ 15,000		19		$ 285,000	Monitor and block scam SMS	$ 3,000		19		$ 57,000
Automate processes to share information		26	19	$ 74	$ 36,744	Share information to verify and block		26	19	$ 74	$ 36,744
Staff training		15	19	$ 74	$ 21,198	Staff training		10	19	$ 74	$ 14,132
TOTAL					**$ 342,942**	**TOTAL**					**$ 107,876**
Very small CSPs						**Very small CSPs**					
Automate manual systems to monitor and block for scam SMS	$ 5,000		130		$ 650,000	Monitor and block scam SMS	$ 1,000		130		$ 130,000
Automate processes to share information		26	130	$ 74	$ 251,404	Share information to verify and block		26	130	$ 74	$ 251,404
Staff training		15	130	$ 74	$ 145,041	Staff training		10	130	$ 74	$ 96,694
TOTAL					**$ 1,046,445**	**TOTAL**					**$ 478,098**
	Year 1 total				**$ 9,733,908**	**Year 2 total**					**$ 2,359,710**
	Less 70% discount				**$ 6,813,735**	**Year 2-9 total**					$ 21,237,386
	Equals				**$ 2,920,172**	**(Yr2-9)/9 =**					**$ 2,359,710**
Average annual cost					**$ 2,415,756**						

Relevant facts and assumptions

- 158 mobile C/CSPs provide customer data for connected mobile services to the ACMA. In addition, it is estimated there are 20 aggregators operating in the Australian market.
- For the purposes of this RIS, mobile C/CSPs are categorised as:
  - Large mobile C/CSPs: 3 (over 1 million).
  - Medium mobile CSPs: 26 (100,000 to 1 million).[111]
  - Small mobile CSPs: 19 (10,000 to 99,999).
  - Very small mobile CSPs: 130 (less than 10,000).
- An additional allowance for 20 aggregators will be added to the medium-sized mobile C/CSP class.
- Without aggregator data, the 3 largest carriers contribute the majority of all services (estimated 95%).
- The 3 large mobile C/CSPs incur the greatest costs because of the complexity of their systems and the volume of customers.
- The majority of costs will be incurred in year 1, as mobile C/CSPs may automate current manual processes that monitor for scams delivered by SMS, or align systems with existing measures, as well as build on information sharing with other mobile C/MSPs where scams delivered by SMS are identified.
- Assumption 70% of year 1 system costs would have been incurred irrespective of the enforceable obligations being imposed to meet existing RSC code obligations or security measures.
- Costs in year 2 onwards drop significantly and mainly accrue in responding to other mobile C/CSPs identifying scams delivered by SMS delivered by that provider. Given the work undertaken in year 1, it is assumed the processes will improve with staff being more experienced, systems streamlined and that the volume of SMS requiring action decreases
- OBPR labour rate of $74.38 adopted (OBPR March 2020 regulatory burden measurement framework – guidance note).

[111]Six mobile providers qualified as medium MCSPs. The ACMA does not receive aggregator data but has assumed an additional 20 MCSPs in the form of aggregators may incur similar costs to a medium sized MCSP. This will be dependent on the substance of regulations introduced.

Appendix B: Calculations to inform the likely annual net benefit over 10 years

Data

	Monetary Loss	Reported w/ Financial Lo	Number of Scams Reporte	Average Loss	Average Loss of Reporting F/L
SMS scams 2021	$ 10,099,886	8.9%	67,180	$ 150	$ 1,689

Assumptions

Increase in losses due to scams	25%
Discount rate	7%
Hours needed to address ID theft	33
Leisure labour rate	$32
Education campaign cost	$41,500
SMS scam incidents with F/L in Year 1	5979
SMS scam incidents in Year 1	67,180
Regulatory Costs - Year 1 (discounting for sunk co	$2,920,172
Regulatory Costs - Year 2 onwards	$2,359,710

Consumers

Year	1	2	3	4	5	6	7	8	9	10
SMS scam incidents - all	67180	83975	104969	131211	164014	205017	256271	320339	400424	500530
SMS scam incidents with F/L	5979	7474	9342	11678	14597	18246	22808	28510	35638	44547

Summary

		Status Quo	Education Campaign			Enforceable Obligations		
			Low	Medium	High	Low	Medium	High
	Intervention Effectiveness		0.1	0.15	0.2	0.6	0.7	0.8
Cost	Direct Costs of Scam Activity	$ 22,420,425	$ 22,420,425	$ 22,420,425	$ 22,420,425	$ 22,420,425	$ 22,420,425	$ 22,420,425
Cost	Time Cost of Scam Activity	$ 157,482,658	$ 157,482,658	$ 157,482,658	$ 157,482,658	$ 157,482,658	$ 157,482,658	$ 157,482,658
Cost	Regulatory Cost	$ -	$ -	$ -	$ -	$ 1,829,423	$ 1,829,423	$ 1,829,423
Cost	Education Campaign Cost	$ -	$ 31,188	$ 31,188	$ 31,188	$ -	$ -	$ -
Benefit	Reduced Fraud	$ -	$ 2,242,042	$ 3,363,064	$ 4,484,085	$ 13,452,255	$ 15,694,297	$ 17,936,340
Benefit	Reduced Time Costs	$ -	$ 15,748,266	$ 23,622,399	$ 31,496,532	$ 94,489,595	$ 110,237,860	$ 125,986,126
	Total status quo cost	$ 179,903,082	$ 179,903,082	$ 179,903,082	$ 179,903,082	$ 179,903,082	$ 179,903,082	$ 179,903,082
	Total incremental cost (present value at 7%)		$ 31,188	$ 31,188	$ 31,188	$ 1,829,423	$ 1,829,423	$ 1,829,423
	Total incremental benefit (present value at 7%)		$ 17,990,308	$ 26,985,462	$ 35,980,616	$ 107,941,849	$ 125,932,158	$ 143,922,466
	Net incremental benefits (present value at 7%)		$ 17,959,120	$ 26,954,274	$ 35,949,428	$ 106,112,427	$ 124,102,735	$ 142,093,043
	Benefit to cost ratio		577	865	1,154	59	69	79

DISCOUNTED DOLLARS

Option 1: Status Quo

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Direct Costs of Scam Activity	$ 10,099,852	$ 11,798,893	$ 13,783,753	$ 16,102,515	$ 18,811,350	$ 21,975,876	$ 25,672,752	$ 29,991,533	$ 35,036,838	$ 40,930,885	$ 22,420,425
Cost	Time Cost of Scam Activity	$ 70,942,080	$ 82,876,262	$ 96,818,063	$ 113,105,213	$ 132,132,259	$ 154,360,115	$ 180,327,238	$ 210,662,661	$ 246,101,239	$ 287,501,448	$ 157,482,658

Option 2: Education Campaign

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Cost of Education Campaign	$ 41,500	$ 38,785	$ 36,248	$ 33,876	$ 31,660	$ 29,589	$ 27,653	$ 25,844	$ 24,153	$ 22,573	$ 31,188
Benefit	Reduced Fraud	$ 1,514,978	$ 1,769,834	$ 2,067,563	$ 2,415,377	$ 2,821,702	$ 3,296,381	$ 3,850,913	$ 4,498,730	$ 5,255,526	$ 6,139,633	$ 3,363,064
Benefit	Reduced Time Costs	$ 10,641,312	$ 12,431,439	$ 14,522,709	$ 16,965,782	$ 19,819,839	$ 23,154,017	$ 27,049,086	$ 31,599,399	$ 36,915,186	$ 43,125,217	$ 23,622,399

Option 3: Enforceable Obligations

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Regulatory Costs	$ 2,920,172	$ 2,205,336	$ 2,061,062	$ 1,926,226	$ 1,800,211	$ 1,682,440	$ 1,572,374	$ 1,469,509	$ 1,373,372	$ 1,283,526	$ 1,829,423
Benefit	Reduced Fraud	$ 7,069,897	$ 8,259,225	$ 9,648,627	$ 11,271,761	$ 13,167,945	$ 15,383,113	$ 17,970,927	$ 20,994,073	$ 24,525,786	$ 28,651,620	$ 15,694,297
Benefit	Reduced Time Costs	$ 49,659,456	$ 58,013,383	$ 67,772,644	$ 79,173,649	$ 92,492,581	$ 108,052,081	$ 126,229,066	$ 147,463,862	$ 172,270,867	$ 201,251,013	$ 110,237,860