Australian Government

acma

Australian Communications and Media Authority

# Reducing the impact of scam calls

## Regulation Impact Statement

DECEMBER 2020

**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

# Contents (Continued)

# Introduction

The Australian Government wants to minimise scam calls and reduce associated financial loss and hardship to consumers. Scams are a whole-of-community problem, and government, industry and consumers all have a role in mitigating associated detriments.

Scammers perpetrate their crimes via a range of obfuscation techniques and scam types such as trying to steal money or identity through phone calls from live operators or robocalls.

Scams over telecommunications networks are a significant problem – not only causing financial and emotional harm to victims but also undermining confidence in telecommunications networks.

Scammers are finding new ways to target Australian telephone customers. They are technologically adept, increasingly sophisticated and show no signs of stopping.

The Australian Communications and Media Authority (the ACMA) is seeking to reduce the harm and loss to Australians caused by scam calls.

This will help prevent financial loss to Australian consumers and promote greater confidence in telecommunication services – no matter which phone provider a customer uses.

# 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.

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

## Current measures for scam calls

Under the Act, two main types of organisations are involved in the provision of services to the public – carriers and carriage service providers (C/CSPs).[1] They play a frontline role in current phone scam disruption approaches.

There are no specific regulatory obligations on C/CSPs[2] to reduce scam calls; however, they have an obligation under Part 13 of the Act to do their best to prevent their networks or facilities being used in the commission of offences against the laws of the Commonwealth, states and territories.

Carriers have complex infrastructure and systems. They own network units that deliver carriage services. Their facilities may include transmission infrastructure, cabling, wireless networks and satellite facilities. Carriers have a large customer base and high traffic volumes and 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 network 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 (VoIP service providers).[4]

Consultation with the telecommunications industry indicated that C/CSPs undertake a range of provider-specific scam reduction activities to block calls and text messages where scam activity can be verified.

[1] ACMA, 'About carriers and carriage service providers', viewed 29 October 2020.

[2] Carriers operate telecommunications networks and infrastructure. Carriage service providers use carrier networks to provide services such as phones and internet.

[3] ACMA, 'About carriers and carriage service providers', viewed 29 October 2020.

[4] ibid.

Communications Alliance Ltd (Communications Alliance), as Australia's peak communications industry body, has undertaken initiatives to address the proliferation of scams on telecommunications networks. In 2016, it published an industry guidance note[5] to clarify the range of uses and abuses of calling line identification[6] (CLI) and how to tackle inappropriate or malicious CLI over-stamping or spoofing[7] as a first step in addressing scams.

Scam calls may over-stamp the CLI of a call (which would generally display the number from which the call originates) to display a number that may be more familiar or recognisable to the person receiving the call. This makes it more likely that the call will be answered.

A prominent recent example of this are scam calls that have a CLI displayed that is associated with the Australian Taxation Office, despite not originating from that number. This scam involves contacting potential victims, with the scammer pretending to represent the ATO and claiming that the person owes money.

It is relatively easy and straightforward to over-stamp the originating number of a call with any number that the caller would like to be displayed. For example, an overseas caller may over-stamp their number with an Australian number. While CLI over-stamping has legitimate purposes (for example, providing a centralised call-back for a call centre, or a doctor who wishes to call a patient from a personal phone but have the practice number displayed), the capability is exploited by criminals.

Over the past few years, large C/CSPs representing around 90% of the market share[8] have voluntarily committed to introducing scam reduction initiatives (including implementation of the CLI guidance note) to reduce the volume of telecommunications scams reaching their customers. However, this commitment has not translated to consistent and coordinated action from all providers, nor has it addressed the impact of scams at a network level.

The remaining smaller CSPs – representing approximately 10% of all fixed-line and mobile services – provide services to customers but do not operate networks. Some of these very small CSPs have as few as one service issued to a customer. These CSPs purchase network capacity from carriers to provide services to their customers.

[5] Communications Alliance, 2016, *Industry Guidance Note (IGN009) CLI Management*, viewed 15 June 2020. The government was not involved in drafting the guidance note and compliance with an industry guidance note is not mandatory nor enforceable by the ACMA.

[6] Calling line identification is the public number displayed on an outgoing call. It is used to accurate route the call over telecommunications networks.

[7] CLI or caller ID enables telephone number of calling number to be displayed. C/CSPs use CLI for the routing of telephone calls (for example, for inbound calls) and billing of services. CLI over-stamping or spoofing is a change of CLI to deliberately mask or mislead the call recipient about the identity of the caller. It causes the caller ID to present as a number different from which the call originates. This can be used maliciously to make a call falsely appear to be from a trusted or local source.

[8] For the purposes of this RIS, we have conservatively estimated a maximum of 413 C/CSPs may be covered by enforceable obligations. Four large C/CSPs (Telstra, Optus, TPG and Symbio) have been allocated nearly 90% of all mobile and fixed-line service numbers. The remaining 10% of numbers have been allocated to 409 medium, small and very small C/CSPs.

It is unlikely smaller CSPs will voluntarily adopt measures because they are:

- smaller in size and capability
- not actively engaged with Communications Alliance and the industry guidance it provides
- potentially unaware of their obligations under the Act.

The ACMA is aware that several C/CSPs have adopted, or are in the process of adopting, measures to disrupt or reduce scam calls. These measures include:

- using a range of data sources to identify scam calls
- using network traffic analysis to identify scam calls
- voluntarily implementing innovative action around disruption of specific scam call types, such as blocking 'Wangiri'[9] call-back scam calls from global networks.

[9] The Wangiri scam involves many telephone calls of very short durations (for example, the call may ring once only) to entice a call-back, usually to an overseas number. The short duration of the call means most calls will go unanswered. Return calls incur a high charge – the longer the call, the higher the charge.

# 1. What is the policy problem?

## Scam calls

Scam activity on Australian telecommunications networks is increasingly sophisticated and hard to detect. It generally originates offshore, readily adapts to disruption measures and ruthlessly exploits new opportunities and vulnerabilities. Australia, along with Canada, the United States and Europe, is targeted by scammers on what is effectively an industrial scale.

Scammers perpetrate their crimes via a range of obfuscation techniques and scam types such as phishing[10], dating and romance, investment and false billing, threats to life or of arrest, unexpected prize or lottery, and online shopping scams. These scams rely on what is essentially 'safety in numbers' high-volume calling and can be perpetrated via voice calls, SMS, instant message, voicemail, or even voice chatbots that will speak back to the victim.

Scams calls are perpetrated in two ways:

> scams that rely on a call back

> cold calls where the scam activity occurs during the call, or subsequent calls.

While it is difficult to estimate the percentages of scams delivered in these ways, scams that rely on a call back do not generally involve CLI spoofing. For the scam to work, the number must be legitimately allocated to a C/CSP and issued to a customer for a return call to be made and connect to the scammer.

Scammers seek to steal money, and often their methods involve the collection of personal information and data to commit identity fraud. Scammers fraudulently obtain this through phone calls from live operators or robocalls. Callers often make false promises – such as opportunities to buy products, invest money, or receive free product trials – and the numbers may appear to be from Australian number ranges; however, they will likely be routed from offshore and/or involved over-stamped CLI numbers.

Scammers will look to incentivise individuals to act on something, for example a prize, a grant, unpaid tax, or a computer virus. Some may even threaten legal action or money loss. Scammers will ask the individual to 'prove' who they are or ask for access to their device. The Australian Competition and Consumer Commission's (ACCC) Scamwatch[11] reports that losses to identity theft scams increased by 193% over 2018, with the highest single reported loss for identity theft being $800,000 to a phone porting scam.[12]

Scammers will use personal data to steal identities, open loans, and steal or launder money. Identity crime is a key enabler of serious and organised crime and surveys conducted by the Australian Institute of Criminology (AIC), beginning in 2013, have

[10] Impersonation and gaining trust are a key tactic of phishing scams. Scammers use fake information, trusted/well-known brands and spurious links leading to malware or locations where criminals can steal personal information. When targets respond to the phish, they respond by giving money, resources, or access to the phisher.

[11] The ACCC works with state and territory consumer protection agencies and other government agencies to promote awareness in the community about scams. Scamwatch is run by the ACCC and provides information to consumers and small businesses about how to recognise, avoid and report scams.

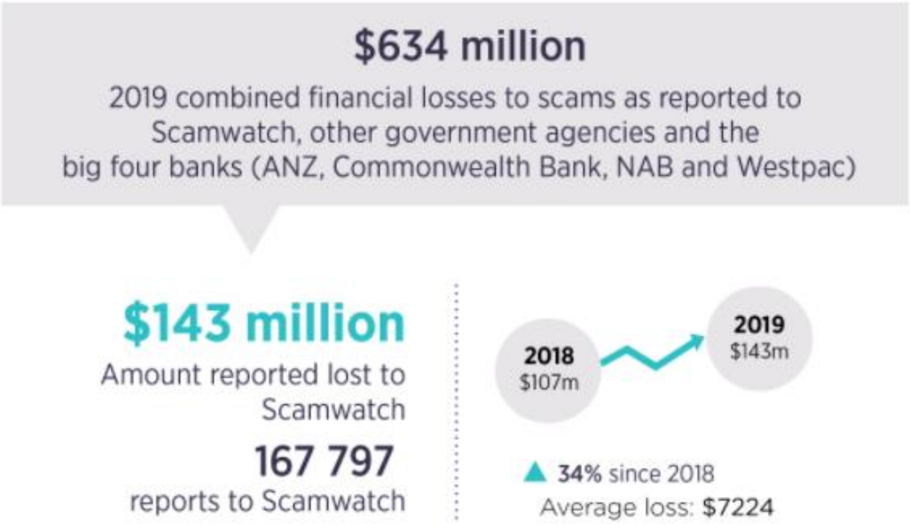
[12] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 6 October 2020.

consistently found that over 20% of respondents' report having experienced misuse of their personal information at some time during their lives.[13]

Criminals use false identities for a variety of reasons, including to:

- perpetrate frauds, including for financial gain such as removing funds from bank accounts
- establish business structures and companies to facilitate other crimes such as money laundering or importing illicit commodities.

## Losses to scams



$634 million

2019 combined financial losses to scams as reported to Scamwatch, other government agencies and the big four banks (ANZ, Commonwealth Bank, NAB and Westpac)

$143 million

Amount reported lost to Scamwatch

167 797

reports to Scamwatch

▲ 34% since 2018

Average loss: $7224

*Source: ACCC Scamwatch, Targeting scams 2019: A review of scam activity since 2009.*

According to Scamwatch, Australians lost over $634 million to scams in 2019 – and there were more than 353,000 combined reports to it, other government agencies and the big 4 banks. These losses are a 34% increase on the previous year.[14]

Based on the combined data, the greatest losses in 2019 by type of scam were:

- $132 million lost to business email compromise scams
- $126 million lost to investment scams
- $83 million lost to dating and romance scams.[15]

In 2019, the number of scam reports to one agency (Scamwatch) was 167,795 – with losses of $143 million. The average reported to Scamwatch increased by 20% to $7,224, up from to $5,997 in 2018.[16]

This year has also seen scammers use events such as the Australian bushfires and coronavirus (COVID-19) pandemic to target Australians. Since March 2020, over

[13] Australian Institute of Criminology, 2019, *Identity crime and misuse in Australia*, viewed 29 October 2020.

[14] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 6 October 2020.

[15] Reported to Scamwatch, other government agencies and the big four banks. ACCC Scamwatch, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 14 October 2020.

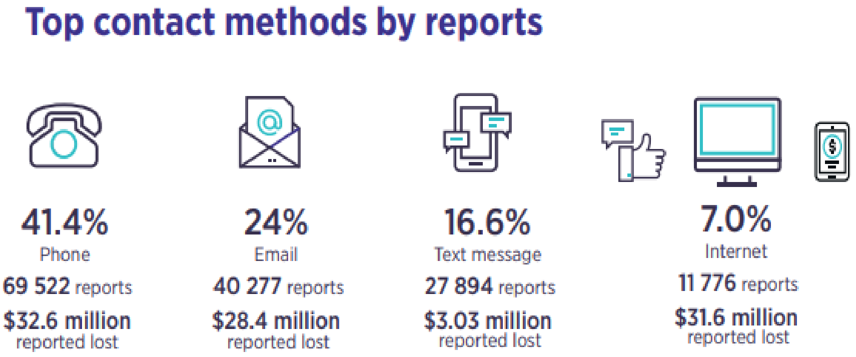
[16] ibid, viewed 5 July 2020.

4,560 scam reports referencing COVID-19 have been reported to Scamwatch, with over $5.1 million in reported losses.[17]

As of September 2020, Scamwatch data shows it received 147, 294 reports of scams from the Australian community, with over $116.5 million in reported losses – suggesting the figure is on track to surpass 2019.[18]

## Losses via phones

Scams occur via several contact methods, but via phone remains the preferred contact method of scammers.



*Source: ACCC Scamwatch, Targeting scams 2019: A review of scam activity since 2009.*

- Over 41% of all Scamwatch reports in 2019 involved scammers contacting Australians via phone – 69,522 reports.
  - 1,856 (2.67%) reports were made by businesses.[19]
- Scams via phone generated more than $32.6 million in reported losses in 2019.
- Of the 69,522 reports of scammers contacting Australians via phone, 2,776 reports cited financial losses occurred with an average loss of $11,737.[20]
  Of these:
  - 2,684 reports were made by individuals (or non-business), with an average loss of $11,724 per reported scam
  - 92 reports were made by businesses and resulted in losses totalling over $1.1million, averaging $11,957 per reported scam.[21]

ACMA data further confirms that Australians are being targeted by scammers on a significant scale. In 2019–20, there were over 11,000 known scams reported to the ACMA, an 11% increase on 2018–20 (9,903 scams reported).[22] Scam calls also constitute the largest category of consumer complaints made to the ACMA across its remit by a significant margin.[23]

[17] ACCC Scamwatch, Current COVID-19 (coronavirus) scams, viewed 14 October 2020.

[18] ACCC Scamwatch, Scam statistics September 2020, viewed 6 October 2020.

[19] Unpublished ACCC Scamwatch data supplied.

[20] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 5 July 2020.

[21] Unpublished ACCC Scamwatch data supplied.

[22] Internal ACMA data based on complaints received from consumers relating to phone scams.

[23] Approximately 30 to 60% of complaints to the ACMA about telemarketing are likely to be about scam calls (due to the activity and obfuscation involved, it is not possible to quantify the figures further).

ACCC's Scamwatch data for 2020 shows that as of September 2020, 42% of all scam reports and 26% of all losses have been from scams received by phone:

- 62,434 reports of phone scams (147,294 total scams reported)
- $31.977 million of the $116.5 million reported in financial losses.[24]

This demonstrates that scams via phone reported remain a significant and growing problem.

## Who is affected by scam calls?

Anyone can fall prey to a scam, regardless of age, gender, education or economic background. Being scammed via a call can happen to anyone who has been issued a local or mobile phone number[25], meaning all Australian telephone users are at risk of financial and associated losses from scam calls.

Access to telecommunications is deeply ingrained in the way Australians live, work and play. It is a constant of modern technology. In June 2019, there were 7.82 million fixed-line phone services and 35.82 million mobile voice services in operation in Australia.[26] In the first half of 2020, ACMA consumer survey data showed that 98% of Australian adults had used a mobile phone to make a call, 92% had sent a text message and 77% had used a messaging/calling application.[27]

While Scamwatch is the primary government website used by Australians to report scams, it is estimated only around 13% of all victims of scams will make a report to Scamwatch.[28]

Consumer losses are almost certainly under-reported as many victims are embarrassed by falling victim to scams. Scam victims may report their experiences in many ways – from discussing what occurred with family and friends, through to reporting to consumer protection agencies and business organisations, and to official reporting to police and regulators. Victims may report to one or all the government or consumer agencies that take reports, such as the ACMA, ACCC, Telecommunications Industry Ombudsman (TIO), IDCARE[29] and the Australian Cyber Security Centre (ACSC).[30] 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. [31]

[24] ACCC, Scamwatch statistics September 2020, viewed 6 October 2020.

[25] Australian local numbers start with the area code (02), (03), (07) or (08). Mobile numbers start with (04XX).

[26] ACMA, 2020, *Communications report 2018–19*, viewed 2 September 2020.

[27] ACMA, 2020, *Trends in online behaviour and technology usage: ACMA consumer survey 2020*, viewed 8 October 2020.

[28] ibid.

[29] 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.

[30] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009,* viewed 13 October 2020.

[31] Australian Institute of Criminology, 2019, 'Identity crime and misuse in Australia', viewed 29 October 2020.

Around 33% of people who had lost money to scams in the previous 5 years did not report that loss to any organisation – resulting in financial losses to scams being grossly understated.[32]

This means the true scale of the impact of scams in Australia is likely far higher than thought because a third of all scams go unreported to any organisation.

In addition, there is no uniform terminology when it comes to scams. Government agencies and other organisations all use different terms to describe different types of scams, which can make comparing data challenging.[33]

As the telecommunications regulator, the ACMA's focus is identifying and addressing solutions to voice and/or robocall phone scams received by Australians on their fixed-line or mobile phone.

Businesses, especially small to medium-sized businesses, face all the same scam risks as individuals. However, several scams specifically target businesses. The most common of these reported to Scamwatch are false billing and phishing scams, while business email compromise scams are the most financially harmful scam affecting Australian businesses.[34]

In 2019, Scamwatch data indicates the greatest losses by type of scam was business – with combined losses of $132 million.[35] However, the losses reported directly to Scamwatch dropped by 27% in 2019, which could be because businesses that sustain substantial losses from scams are likely to report the matter directly to the police and/or their banks.

For the 92 businesses that did report losing money from scams via phones, losses totalled over $1.1 million, with an average loss of $11,957.

Alongside financial losses from scams, identity crime continues to affect a large number of Australians, as well as businesses and government agencies. The estimated direct and indirect cost of identity crime in Australia in 2018–19 was $3.1 billion – an increase of 17% from 2015–16.[36]

Consumers who are the victim of identity theft typically suffer both financial loss and psychological harms. The effects can be life-altering, impacting health, emotional wellbeing, and relationships with others.[37]

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.[38] In figures for 2017–18, IDCARE estimated that an average of 32 hours is spent by customers to address identity theft.[39] These figures do

[32] ACCC, 2020, *Targeting Scams 2019 A review of scam activity since 2009*, viewed 13 October 2020.

[33] ibid.

[34] ibid, viewed 21 October 2020.

[35] Combined losses reported to Scamwatch, other government agencies and the big four banks. ibid, viewed 14 October 2020.

[36] Australian Institute of Criminology, 2019, 'Identity crime and misuse in Australia', viewed 29 October 2020.

[37] Identity Theft Resource Centre, 2018, '*The Aftermath – the non-economic impacts of identity theft*', viewed 9 October 2020.

[38] IDCARE unpublished data supplied to Australian Institute of Criminology for 'Identity crime and misuse in Australia', 2019, viewed 29 October 2020.

[39] IDCARE, 'Unauthorised Mobile Phone Porting Events', IDCARE Insights bulletin 2018.

not include lost productivity, where a customer has taken time off work to address identity theft. The emotional distress caused by scams can also be devastating.

As support charity Life After Scams states:

> Behind these mind-boggling statistics are real human beings, who are crippled by debt, traumatised by their ordeal and stuck wondering how to rebuild their lives.[40]

The government's policy objective is to reduce scam calls occurring, given the significant potential for consumer harm. Scam activity impacts directly on the financial and emotional wellbeing of many Australians. It also undermines confidence in our telecommunications services. In this sense, C/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.

[40] Productivity Commission, 2019, 'Life After Scams Submission to Productivity Commission', viewed 14 October 2020.

# 2. Why is government action needed?

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.

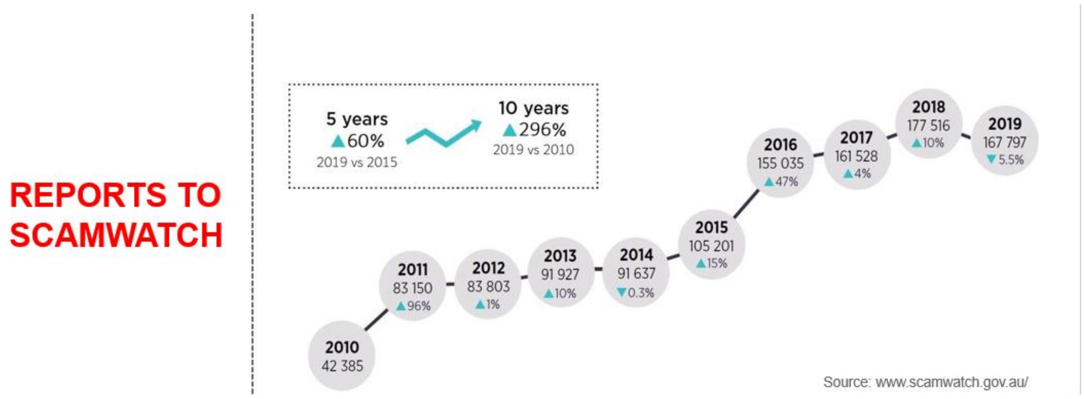
Emerging technologies have also resulted in a greater consumer expectation that access to those technologies and services is appropriately safeguarded from harms.

Consultation with the telecommunications industry has indicated a range of C/CSP-level scam reduction activities are undertaken on a regular basis. These involve blocking scam calls where they can be verified, primarily via customer complaints indicating calls are scam activity.

Some C/CSPs are undertaking innovative action around disruption of specific scam call types, such as blocking Wangiri call-back scam calls, identifying and blocking high volume call activity and working with government agencies (like the Australian Tax Office) to reduce the impact of scams targeting the particular government brand.[41]

While these C/CSP-level approaches are laudable, they are largely ad hoc and relatively small scale, given the volume of scam traffic reported as being carried on Australian telecommunication networks and the harm it causes. In addition, not all providers have acted to adopt measures to reduce scam calls, and that gap creates further opportunities for scammers, which has consequences for all consumers.

As the following ACCC data indicates, reports of scam activity have been increasing over the 10 years since 2010, demonstrating market failure. Government action is required to address the growing consumer detriment.



Source: www.scamwatch.gov.au/

Putting clear and enforceable information/data sharing obligations in place will support coordinated scam reduction initiatives. Currently, it is generally easier for C/CSPs to share information with a government agency than it is for them to share between each other. C/CSPs have obligations to protect information under the *Privacy Act 1988* as well as under Part 6 of the Act. C/CSPs also view the relationship with their customers as commercially sensitive and want to protect their customer base.

[41] Joint media release: Ministers Fletcher and Sukkar, ‘Stopping ATO phone call scams’, 9 May 2020, viewed 14 October 2020.

Motivated scammers will always find ways to exploit new and existing business processes and technologies. The potential for scam traffic to circumvent C/CSP level blocks (including by moving activity to another provider), means there is a need for industry-wide solutions to be developed and adopted.

More can be done to address the problem of scam calls – requiring C/CSPs to collaborate, cooperate and share information to disrupt scam calls provides the strongest incentive to achieving the best outcome for the Australian community.

## Combating scam calls

Combating telecommunications scams is a government priority, and multiple government and law enforcement agencies receive reports of scam activity. The ACMA has a key role as the regulator of the telecommunications industry and unsolicited communications (commercial electronic marketing and telemarketing).

Other key agencies include the ACCC as the competition regulator, the ACSC as the Australian Government lead on cyber security issues, and the Australian Federal Police and other law enforcement agencies in relation to perpetrated scams.

ACMA consumer research confirms scams over telecommunications networks are a significant problem, and consumers expect more to be done by government.[42] International experience and submissions to the ACMA's Scam Technology Project discussion paper indicate that there is no single or simple solution to combating phone scams. For example, basic provider-level call blocking is a reactive, 'whack-a-mole' exercise where scammers often immediately present a new maliciously spoofed CLI. [43]

Analysis of stakeholder feedback, the domestic context and international approaches indicates that technological solutions to scam disruption need to sit within a broader framework to be effective.

In November 2019, the Minister for Communications, Cyber Safety and the Arts endorsed the ACMA's *Combating scams action plan*. One of the key recommendations of the action plan was for the development of enforceable obligations for C/CSPs to:

- share scam call data across industry
- verify, trace and block scam calls
- prevent carriage of domestic originating calls where the caller does not hold the rights of use to the number
- minimise carriage of international originating calls using illegitimate CLI
- refer scam calls and/or perpetrators to authorities.

### Enforceable obligations

Under Part 6 of the Act, the enforceable obligations options available to the ACMA are either an industry code or an industry standard.

[42] ACMA, 2018, *Unsolicited calls in Australia: Consumer experience,* viewed 2 October 2020.

[43] 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. The *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 three-point *Combating scams action plan.*

The ACMA 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 the ACMA is directed to make such an instrument by the minister administering the Act.

Placing obligations in an industry code provides the ACMA with lower-level enforcement powers if C/CSP non-compliance is found; that is, a formal warning or direction to comply with the code.

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 Act).

Compliance with an industry standard is mandatory. An industry standard requires the section of the industry to which the code applies to meet obligations. If a C/CSP contravenes a standard, the ACMA may:

- issue a formal warning (section 129)
- give a remedial direction (sub-section 69/102)
- accept an enforceable undertaking (Part 31A)
- give an infringement notice (Part 31B)
- seek an injunction in the Federal Court which would compel the person to act or refrain from acting in a particular way (Part 30)
- seek civil penalties via Federal Court proceedings (up to $50,000 for a person and $250,000 for a body corporate per contravention) (Part 31).

# 3. What policy options have been considered?

The policy options below are consistent with regulatory options available in accordance with the Act.

## Option 1: Non-regulatory option (status quo)

The government continues to encourage the telecommunications industry to implement scam call mitigation measures and provides general advice to consumers on avoiding scams (for example, through Scamwatch and ACMA resources setting out how consumers can protect themselves). The existing legislation and regulations for C/CSPs remain – including obligations under Part 13 of the Act.

Communications Alliance encourages C/CSPs to act in accordance with the industry CLI guidance note, with members deciding whether to voluntarily comply. Those providers deploying scam mitigation measures continue to use them in addition to existing laws and regulations to help reduce instances of scam calls.

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

No compliance requirements or enforcement options would apply. Scam calls will still reach consumers and it is likely the volume of calls and harms escalate as no coordinated, industry-wide technological or network strategies have been deployed.

## Option 2: Consumer education campaign

The government does not introduce any new form of regulation but conducts a targeted public education campaign that provides clear and accessible information to assist consumers to better manage and avoid scam calls. The existing legislation and regulations governing C/CSPs remain.

The campaign advises customers how to improve their phone security and what to do if they become a victim of a scam call – including where to report it.

Information is provided to C/CSPs to further support their understanding of the current regulatory framework so they act in a manner that will minimise the need for further regulatory intervention. Better informed customers pressure C/CSPs to go beyond existing regulation and voluntarily implement additional protections.

Campaign activities are also undertaken in collaboration with other government agencies, consumer advocacy groups and 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 culturally and linguistically diverse communities and vulnerable consumers (such as older Australians and First Nations Australians) to inform and help them better manage scam calls. However, some members of the community may still not receive nor understand the campaign information.

The campaign is run annually for 10 years by the ACMA in accordance with usual practice and builds on other campaigns. A campaign based upon the below steps will cost on average $30,000 per annum (depending on the size of the intended audience):

- information on the ACMA and other government websites
- a short, engaging video providing individuals and business with relevant information in an accessible format
- poster campaign focusing on information for vulnerable communities including translations into multiple languages
- design targeted to First Nations Australians audience
- targeted ads on Facebook to reach consumers (including an image, content and link back to the ACMA website)
- use of LinkedIn to reach business and C/CSPs
- use of direct email lists and line area industry contacts
- boosting impressions of the social media content (potentially reaching 7.7m people).

This option relies entirely on better informed consumers reacting appropriately to identify and manage scam calls.

## Option 3: Enforceable obligations

The government introduces enforceable obligations under Part 6 of the Act to reduce scam calls. This includes establishing industry-level consistent, flexible, and operationally-sound processes for C/CSPs to use to verify, trace and block scam calls by all C/CSPs.

A C/CSP would be required to:

- provide up-to-date guidance material on its website to assist its customers better manage scam calls
- interrogate its systems to:
  - identify high-volume, short duration calls from a particular CLI or range of CLIs
  - block calls presenting with problematic CLI (for example, use of numbers inconsistent with the Telecommunications Numbering Plan 2015)
  - ensure its customers are presenting calls with the CLI legitimately issued to them (instead of CLI spoofing)
  - block internationally originating calls presenting with Australian numbers (except in limited circumstances)
  - trace scam calls originating from its customers when referred by another C/CSP
  - share information in an agreed format with other C/CSPs to reduce scam calls
  - use contractual arrangements with international operators to block internationally-originating scam calls reaching Australia.

This option proposes enforceable obligations be principle or outcomes-based to avoid providing sensitive information to scammers, while ensuring they permit adaptive and flexible initiatives to address scams and/or do not stifle potential innovation.

This option provides the ACMA with powers under Part 6 of the Act to take action to ensure C/CSPs comply with enforceable obligations.

Enforcement action against overseas scammers may be achieved where quality intelligence can be provided to relevant law enforcement agencies through appropriate channels.

# 4. 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 for 10 years
- future costs/benefits are discounted to present value using a discount rate of 7%
- costs and benefits are reported in average annual figures.

## Option 1: Status quo

### Benefits

If the status quo is maintained, the Australian community will continue to be subject to scam calls, as scammers can target any Australian mobile, landline or business service number.

C/CSPs that have not implemented monitoring, verifying, tracing and scam call data-sharing may benefit from choosing not to implement any additional processes beyond what is currently required to meet existing obligations under Part 13 of the Act, although it is noted that such a provider may be subject to reputational and lack of consumer confidence issues.

### Costs

This option does not generally impose any additional regulatory costs on consumers, businesses, or C/CSPs.

The impact of scam calls on the Australian community is serious and includes (but is not limited to) financial loss, negative credit ratings, psychological harm and emotional stress. If the status quo is maintained, it can be assumed that the levels of harm attributed to the impact of scam calls will continue to increase as scammers become more efficient at targeting customers.

As reported by Scamwatch, in 2019, Australians made 167,797 scam reports, and financial losses increased by 34% from 2018:

- Of these, scams via phone accounted for 41% of all scams (69,522 reports) and more than $32.6 million in reported losses.
- This is an increase of over 7% on losses to scams via phone in 2018.[44]

It is important to note that these reports and losses continue despite some C/CSPs voluntarily implementing scam disruption measures.

Scamwatch research also shows that scams are both under-reported (by approximately 33%) and inconsistently reported – victims may report to none, one or all the government or consumer agencies that take reports.

Therefore, for the purposes of this RIS, a conservative average annual increase of 7% has been applied. This considers that from 2018 to 2019, there was an increase in reports of losses from scams via phone of 7%, while reported scams via phone accounted for 41% of all losses in 2019. As of September 2020, 42% of all reports to Scamwatch in 2020 have been about scams received by phone – this is up slightly

[44] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 6 October 2020.

from 2019 and accounts for nearly the same in losses – yet with 3 months of the year to go.

It can be anticipated that if the status quo remained, losses from reported scam calls to consumers and business would continue to increase, and there would be, on average, $35.3 million in direct financial losses each year over a 10-year period.[45]

Assuming customers quickly notify their financial institution, the financial cost of fraud may be borne by those institutions – with customers recovering money lost through fraud protection policies. However, the costs borne by financial institutions will either increase insurance costs and/or be recovered across the customer base.

In addition, while scam victims may, ultimately, recoup financial losses, identity theft victims may experience similar emotional effects as victims of violent crimes, ranging from anxiety to emotional volatility. Once someone has had their identity stolen, it can be very difficult and time-consuming to reverse the effects.[46]

Customers who have had their identity stolen need to spend time addressing their losses (both financial and of their identity) and may use support services to assist them. For example, they may seek advice from IDCARE before contacting government services that might be compromised (such as myGov, ATO, Medicare), their financial institutions (banks, superannuation, investment firms) and their C/CSP.

Taking the IDCARE figures for 2017–18 that estimate an average of 32 hours is spent by people to address identity theft, this represents a minimum cost of $1,024 per victim – or total losses of $2,748,416 per year (calculated at the OBPR leisure labour rate of $32 per hour for private citizens and based on an estimate of 2,684 reports in 2020).

Victims of identity theft can also experience multiple instances of fraud over months or years.[47] Support service IDCARE recommends victims set up yearly reporting to allow for continual monitoring. Identity theft has long-term, unquantifiable repercussions for victims.

But the impact phone scams have on individuals whose identity is stolen goes beyond economic losses suffered. Identity theft affects more than just any single individual. The fraud can impact those close to victims, with financial and psychological stress involved.[48] In some extreme cases, victims have difficulties in finding employment, are refused services, or are refused credit due to the fraud.[49]

In a survey conducted by the Identity Theft Resource Centre, victims reported significant distress well beyond the initial instance of fraud. They reported feelings of anxiety, anger and frustration, violation, powerlessness and sadness. These feelings result in physical consequences including problems with sleep, increased stress levels, concentration issues, persistent aches, pains or headaches and fatigue.

As scam calls can target any landline or business number, the costs to business from financial losses from scam calls is generally considered to be higher. The 92 reports of losses from scams via phone made by businesses in 2019 totalled $1.1 million, with an average loss of $ 11,957. This is significantly higher than the average loss reported

[45] Compound growth on $32.6m over 10 years discounted at 7% each year.

[46] Identity Theft Resource Centre, 2018, *The aftermath – the non-economic impacts of identity theft*, viewed 9 October 2020.

[47] Australian Institute of Criminology, 2019, *Identity crime and misuse in Australia*, viewed 9 October 2020.

[48] Identity Theft Resource Centre, 2018, *The aftermath – the non-economic impacts of identity theft*, viewed 9 October 2020.

[49] Australian Institute of Criminology, 2019, *Identity crime and misuse in Australia*, viewed 9 October 2020.

to Scamwatch in 2019 across all contact methods ($7,224).[50] Scamwatch data also indicates the businesses had the highest combined losses of $132 million in 2019.[51]

There is evidence that a business, which has its legitimately-issued number illegally spoofed by scammers, will lose time and money rectifying the issue.[52] In some cases, a business may need to arrange a new telephone number with their provider, which has flow-on effects for their business (including changing marketing materials, systems and informing existing customers).

## Option 2: Consumer education campaign

### Benefits

There are no direct costs to individuals or business from an education campaign. An education campaign will support the Australian community to be more aware of how to identify and manage scam calls.

Informed consumers are more likely to better protect their personal information, which will help prevent harms being perpetrated, including identity theft – and reduce the significant distress, trauma and suffering that occurs due to scammers. In 2019, Scamwatch heard from many scam targets who avoided becoming victims simply because they told someone about their experience, and that person advised them that it sounded like a scam.[53]

Consumers will be empowered to protect themselves from scam calls and know how to respond in the event of receiving one – for example, by taking control of how they share their personal information in public and quickly contacting their financial institution or reporting it to Scamwatch.

The continuation of education and awareness campaigns about phone scams may increase reports as more people learn from government campaigns how to spot and stop a scam call. Over time, there has been a shift from reports of scams seeking money to reports about scams seeking information.[54] An informed individual is more likely to better protect their personal information, which will help reduce the harms associated with scam calls.

Well-informed decisions are vital in encouraging competition and driving providers to operate efficiently. Informed customers will actively seek the best protection for themselves and may ask providers what they are doing to reduce scam calls before choosing their provider.

This may incentivise C/CSPs to voluntarily increase protections in accordance with the status quo, which may also reduce instances of scam calls. Better informed consumers will drive more providers to view voluntary additional protections as aligned to their existing obligations, that is, part of their duty to do their best to prevent their networks or facilities being used in commission of criminal activity. For example, a provider that voluntarily implements scam disruption measures by blocking suspicious call activity may stop thousands of consumers being targeted.

[50] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 6 October 2020.

[51] Reported to Scamwatch, other government agencies and the big four banks. ibid, viewed 14 October 2020.

[52] ABC News, 2019, 'Phone spoofing: When your phone number is taken over by international scammers', viewed 5 October 2020.

[53] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 16 October 2020.

[54] ibid.

An educational campaign would have reputational benefits for the telecommunications industry – particularly for providers that can demonstrate their commitment to protections for their customers. C/CSPs that adopt good practices have a competitive advantage by being able to advertise themselves as being the provider that protects consumers.

Education campaign activities will enhance a provider's (particularly smaller providers) understanding of their regulatory responsibilities to both consumer and the regulator. Stronger application of existing industry CLI guidelines may also reduce instances of identity theft.

The practical impact of an education campaign could result in an estimated 20 to 30% reduction in the impact of scam calls compared to the status quo. This reduction is due to the increase in voluntary protections and the impact of informed and proactive consumers in reducing the impact of scam calls. However, information provision alone does not create long-lasting behaviour change, and the campaign would have to be re-run multiple times for it to have sustained benefit.

The initial benefits of this reduction represent:

- a decrease of 20 to 30% in instances of psychological harm caused by identity theft from scam calls, and the need for consumers to seek support services
- prevention of financial losses to scam calls of between $5.2 million and $7.9 million each year comprising:
    - direct savings to consumers of between $4.7 million and $7 million[55]
    - savings in time spent by customers responding to identity theft of between $413,000 and $619,000[56]
    - reduction in losses to business of between $165,000 and $248,000.[57]
- freeing up of financial institution and/or telecommunication fraud team[58] resources by 20 to 30% 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 relating to scam calls (equivalent savings of 20 to 30%).

### Costs

Better informed customers may also increase workloads for fraud teams – as customers will be more responsive to the signs of scam calls. Financial institutions and C/CSPs will continue to need to spend time and resources responding to scam calls, as well as assisting consumers to manage the impact.

C/CSPs may need to direct resources towards implementing additional stakeholder engagement activities and updating existing information to align with campaign activities. This includes additional time spent on training frontline staff or resourcing specialist fraud teams on how to identify and address potential scam calls.

[55] Based on a 20 to 30% reduction in $31.5 million of direct losses to consumers in the status quo.

[56] Figure based on reduced reports * 32 hours * $32 discounted over 10 years.

[57] Figure based on a 20 to 30% reduction in $1.1 million direct losses to business in the status quo.

[58] Stakeholder feedback suggests this is currently equivalent to 20 to 30% of C/CSP fraud team time.

## Option 3: Enforceable obligations

### Benefits

***Consumers***

The Australian community can expect to benefit from the option to introduce enforceable obligations that mandates action to address scam calls and provides increased consumer safeguards.

The most significant benefit from enforceable obligations would be a reduction in the financial impact of scam calls reaching consumers. For this assessment, it is conservatively estimated that enforceable obligations will result in 70% reduction in the impact of scams – depending on the mechanism used to set obligations.

Enforceable obligations have the potential to provide significant positive impacts by reducing the financial and emotional harms that an individual may face from scam calls. They could reduce reported losses from scams via phone by around 2,500 calls annually over the next 10 years, relative to the status quo.

Individuals can expect to benefit from enforceable obligations that enable a flexible, coordinated, and practical approach for industry to adopt actions to address scam calls. Scammers will adapt to technology as quickly as it changes and build knowledge of local environments to impersonate trusted organisations. Scammers are also quick to take advantage of local events and crises. Placing obligations on C/CSPs to collaborate to disrupt scam calls will also provide improved opportunities for referral for regulatory or law enforcement action.

Multiple government and law enforcement agencies receive reports of scam activity. Sharing this scam report data would help C/CSPs improve scam call identification and blocking. As one C/CSP consulted explained:

> We believe there will also be benefit in regulators (and consumer protection agencies) sharing the pertinent details of reported scams with network operators. This would give carriers better evidence of what calls are scams, improving the effectiveness of tracing the source of the scam by reducing false positives.

***C/CSPs***

Enforceable obligations provide the opportunity to encourage consistent, community-wide approaches to combating scam calls by establishing processes and protections that provide certainty for C/CSPs and their customers. With all 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.

C/CSPs can expect to benefit from improved scam call data-sharing across industry, particularly where the provider itself is the victim of an impersonation scam.[59]

Indirectly, C/CSPs and financial institutions will benefit from spending less time and resources responding to complaints about scam calls, as well as assisting consumers to manage the impact.

Additional action by C/CSPs to act against scam calls and share information about scam calls with other providers will become more effective as the market is covered by protections. If all providers are working cooperatively to address scam calls, the Australian communications ecosystem is better protected.

[59] Sydney Morning Herald, 27 August 2018, 'Scammers pretend they're from Telstra, ATO, Centrelink to steal money', viewed 8 October 2020.

The benefits of this reduction represent:

- a 70% decrease in instances of psychological harm caused by identity theft from scam calls, and the need for consumers to seek support services
- annual savings from financial losses to scam calls of approximately $18 million comprising:
  - direct savings to consumers of around $16 million[60]
  - annual savings in time spent by customers responding to identity theft of approximately $1.4 million[61]
  - reduction in losses to business of around $600,000[62]
- freeing up of financial institution or telecommunication fraud team resources to assist customers on other matters (equivalent to savings of 70%)
- a reduction in the resources required by community organisations (such as IDCARE) to assist customers who have experienced identity theft relating to scam calls (equivalent to savings of 70%).

A collaborative approach to addressing scam calls provides a reputational benefit for C/CSPs. It demonstrates to consumers that C/CSPs are taking concerted, industry-wide steps to improve consumer safeguards and disrupt scam calls.

Collaborating to reduce scam activity provides positive benefits for providers when their networks and services are viewed as more safe and secure. This benefit accrues from customers who are satisfied with extra protections, as well as businesses who appreciate the secondary protections afforded to their customers through enforceable obligations. In addition, C/CSPs – which are relentlessly targeted by scammers impersonating their brands and attempting to steal the identity of their customers – benefit from the extra protections.

Providers that have tested the proposed obligations can share their experience and expertise to enable a more practicable, robust and technically-feasible requirements to be implemented.

**Costs**

***Consumers***

There are no direct costs to consumers from enforceable obligations; however, the Australian community can expect to benefit from collaborative and coordinated action to address scam calls.

Experience has shown there is no ‘silver bullet’ to address scam calls. Scam calls are difficult to distinguish from legitimate calls as the characteristics of scam calls (such as high volume and short duration) can represent legitimate telecommunication activity (for example, telemarketing calls). Scammers are also able to quickly adapt to changing environments – as seen most recently with scammers taking advantage of the Australian bushfires and then the coronavirus pandemic. For scams involving CLI spoofing, scammers regularly change the calling number displayed, which makes verifying, tracking and blocking difficult and/or ineffective.

Costs to the community come from the residual instances of scam calls, that is, those not reduced by the enforceable obligations, including from the impact from

[60] Based on a 20 to 30% reduction in $31.5 million of direct losses to consumers in the status quo.

[61] Figure based on reduction reports * 32 hours * $32 discounted over 10 years.

[62] Figure based on a 70% reduction in $1.1 million direct losses to business in the status quo.

psychological harm and distress experienced by each victim of a scam call and the ongoing repercussions of identity theft.

***C/CSPs***

Ensuring enforceable obligations are outcomes-based will provide flexibility for C/CSPs in complying. For example, it may be more efficient for carriers and larger carriage service providers to automate their systems, but for a smaller carriage service provider with less customers, the necessary activities could be conducted manually.

Each C/CSP is responsible for determining how they monitor their network to detect and act against scam calls. Communications Alliance has indicated that 30% of costs for systems automation would have accrued to comply with existing obligations.

Where costs accrue under enforceable obligations, costs will be higher for carriers (including carriers operating both fixed and mobile services) due to their role in the telecommunications ecosystem, as carriers provide the basic transmission infrastructure on which carriage and content services are supplied to the public. In addition, carriers operate international gateways carrying internationally-originating traffic (including scam calls) onto domestic networks. Obligations to work with international carriers to reduce scam calls should lessen the burden on the Australian telecommunications industry as a whole.

For the purposes of this RIS, C/CSPs have been characterised as follows (based on the volume of local and mobile service numbers allocated by the ACMA):

- large carriers: 4 (over 10 million numbers)
- medium CSPs: 18 (1 million to 10 million numbers)
- small CSPs: 150 (100,000 to 1 million numbers)
- very small: 241 (1 to 100,000 numbers).

The number of C/CSPs that will be covered by enforceable obligations has been conservatively estimated at a maximum of 413. This maximum includes each C/CSP; however, there are a number of partnerships and carrier relationships in place. For example, some smaller CSPs are owned by larger C/CSPs, while others purchase network capacity to provide services to their customers.

It is anticipated that while all C/CSPs need to have processes to comply with enforceable obligations, some provisions (for example, on information sharing) would only be enlivened when the volume of calls trigger materiality provisions. Similarly, C/CSPs are expected to incur ongoing costs associated with sharing scam call information with other providers and to relevant government agencies. But the requirement to share information with the ACMA and other regulators may only be enlivened where a C/CSP does not respond the notifying C/CSP.

It is also assumed (based on current practice) that while monitoring activities continue in real time, tracing and verifying activities (including information-sharing with other providers) will occur on a weekly basis for large carriers and medium C/CSPs.

As Table 1 below, costs from Year 2 drop significantly and mainly reflect the activity involved in responding to other C/CSPs identifying scam calls delivered by that provider.

**Table 1: Costs to all C/CSPs to comply with enforceable obligations over 10 years**[63]

| Category | Costs: Year 1 | Cost: Year 2 onwards |
|---|---|---|
| Large | $618,116 | $118,116 |
| Medium | $801,524 | $225,524 |
| Small | $1,144,470 | $509,895 |
| Very small | $1,236,282 | $935,032 |
| **Sub-total** | $3,800,392 | $1,808,567 |
| Less 30% Year 1 systems automation costs incurred, irrespective of ongoing obligations | $1,478,217 | |
| **Total** | **$2,322,175** | **$1,808,567** |

Given the work undertaken in Year 1, it is assumed the processes will improve with staff being more experienced, and that the volume of calls requiring tracing action decreases.

Where costs accrue in complying with enforceable obligations, the costs are predominately one-off system development costs such as the implementation of potential new IT systems or procedures, and training staff in those systems.

Scams are an international problem that challenge industry and regulators across the globe. Putting in place scam call disruption measures may potentially divert scammers to other markets or services. However, these other platforms (such as social networking sites) are also the subject of government action. For example, the ACCC is conducting an inquiry into markets for the supply of digital platform services, which includes segments such as online private messaging services, social media services and digital content aggregation platform services.[64] In addition, the Australian Cyber Security Centre (ACSC) has carriage for actions to create a more secure online world for Australians, their businesses and essential services through Australia's Cyber Security Strategy 2020.

Addressing scam calls through enforceable obligations, will make Australia a harder target for scammers overall and have specific benefits such as restoring confidence in the telecommunication networks that underpin the way Australians engage in the modern world. It must be a coordinated approach, or the weakest link will be targeted, which, to this point, is Australians targeted by scam calls.

[63] See Appendix A for a further breakdown of costs.

[64] ACCC, Digital platform services inquiry 2020-2025, viewed 14 October 2020.

## Regulatory burden measurement table

| Option | Regulatory cost (annual) |
|---|---|
| Status quo | n/a |
| Consumer education campaign | n/a |
| Enforceable obligations | $1,410,541 |

We anticipate that the regulatory burden for all C/CSPs to comply with enforceable obligations is around $1.41 million annually for 10 years.

This assumes that:

- 30% of costs for systems automation would have accrued to comply with existing obligations
- costs will be higher for the 4 carriers (including carriers operating both fixed and mobile services)
- IT and systems costs will be predominately one-off
- costs will decrease as processes improve over time.

## Likely annual net 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 (see Appendix B).

| Options summary* | | Option 1: Status quo | Option 2: Education campaign | | Option 3: Enforceable obligations |
|---|---|---:|---:|---:|---:|
| | | | Low | High | High |
| Effectiveness of intervention - % reduction in scam calls | | 0 | 0.2 | 0.3 | 0.7 |
| Cost | Costs to customers (direct) | –$31,467,269 | | | |
| Cost | Costs to customers (time) | –$2,748,416 | | | |
| Cost | Costs to business | –$1,100,366 | | | |
| Cost | Cost of education campaign | | –$30,061 | –$30,061 | |
| Cost | Regulatory costs | | | | –$1,410,541 |
| Benefit | Reduced scam calls to customers | | $4,729,677 | $7,094,515 | $16,553,868 |
| Benefit | Reduced customer time costs | | $413,100 | $619,650 | $1,445,849 |
| Benefit | Reduced scam calls to business | | $165,390 | $248,085 | $578,865 |
| **Net cost/benefit** | | **–$35,316,051** | **$5,278,106** | **$7,932,189** | **$17,168,042** |

** Assumes 7% annual growth in scam calls, 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 C/CSPs that will incur regulatory costs.*

# Who was consulted and what did they say?

## Consultation

The ACMA has been kept informed by Communications Alliance on industry measures to address scam calls over time, including the development of a CLI industry guidance note and other phone scam mitigation activities. The ACMA has regularly sought data to understand the magnitude of the issue and information about any actions taken by carriers to address scam calls.

In 2018, 46.8% of scam reports concerned phone calls.[65] In response to the problem and a request from the then Minister for Communications and the Arts, the ACMA established the cross-agency Scam Technology Project with the ACCC and the ACSC to explore ways to reduce scam activity over telecommunications networks.

The project recognised that effective scam reduction at an industry-wide level can only be achieved through industry and regulators working together to develop improved processes and infrastructure that supports appropriate sharing of scam data and referral for regulatory or law enforcement action.

In March 2019, a public discussion paper was released and extensive targeted consultation with key stakeholders occurred. Through consultation, the ACMA found several specific initiatives and mechanisms that could potentially identify offshore illegitimate traffic to facilitate blocking by C/CSPs.

Submissions informed and shaped the Scam Technology Project and in November 2019, the Minister for Communications, Cyber Safety and the Arts signed off on the project's *Combating scams action plan*. The 3-point action plan included forming a joint government-industry taskforce, developing new enforceable obligations and immediately trialling new scam reduction initiatives.

Following the release of the action plan, the Scam Technology Action Taskforce (STAT) was established to take on responsibility for actions on telecommunications scams. Chaired by the ACMA, STAT includes members from government (the ACCC, ACSC and the Department of Infrastructure, Transport, Regional Development and Communications) as well as Communications Alliance (and its members). Other relevant parties such as law enforcement, government agencies and financial institutions with observer status also participate where issues are relevant to them.

The ACMA met with Communications Alliance to better understand existing industry practices and how they could be reflected in an industry code. The ACMA has similarly engaged with IDCARE and the Australian Communications Consumer Action Network (ACCAN) to understand their view of the problem.

### Release of industry code for public comment

In September 2019, Communications Alliance commenced work on developing an industry code and convened a working committee comprising carriers and carriage service providers. A code, when registered by the ACMA, would place enforceable obligations on C/CSPs to identify, trace and block scam calls. It also looked at introducing disruptive measures through the code which are expected to reduce the

[65] ACCC, 2018, *Targeting scams Report of the ACCC on scams activity 2018*, viewed 23 August 2020.

number of scam calls reaching Australian consumers and help identify scam activity for referral to enforcement agencies.

In March 2020, Communications Alliance released a draft *Reducing Scam Calls* code for public comment with submissions closing in May. The draft code was published on their website and promoted through industry and government channels, mainstream media and social media.

To register a code, the ACMA must be satisfied that Communications Alliance has consulted as per section 117 of the Act. Communications Alliance is required to consult with the ACCC, the Office of the Australian Information Commissioner (OAIC), the Telecommunications Industry Ombudsman (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 provided evidence to the ACMA to substantiate that appropriate consultation was undertaken with ACCAN, the ACCC, OAIC and the TIO.

As per section 117 of the Act, the ACMA must also consult with the OAIC that it is satisfied with the code – particularly if it deals with matters under the *Privacy Act 1988*. The ACMA consulted OAIC and received confirmation that OAIC was satisfied with the code.

The ACMA is satisfied that Communications Alliance met its consultation requirements as per section 117 of the Act.

### Summary of stakeholder feedback

Seven submissions were received in response to the draft code. All submissions supported an industry code being made to address scam calls.

Key submission themes included:

- clarification of the objectives of the code
- practical technical amendments suggested by C/CSPs
- timeframes for actions in the code
- recognition of the importance of:
  - information sharing, ideally in a centralised system
  - providing consumer awareness information
- suggestion that the code contains a commitment to combat SMS scams and monitor international best practice scam mitigation strategies
- role of the TIO – for example, it may consider obligations under the code when determining a fair and reasonable outcome of a scam complaint.

The ACMA was represented on the Communications Alliance working committee as an observer. We can attest that the working group considered all submissions made, noting that several matters were subsequently revised within the code, including technical considerations such as the need for consideration of international mobile roaming in the context of legitimate use of CLI.

# What is the best option from those considered?

Scammers are technologically adept, increasingly sophisticated and show no signs of stopping. This emphasises the need for government to encourage practical technological solutions that increase the effectiveness of preventing and disrupting scam call activity on Australian telecommunication networks. Enforceable obligations determined under Part 6 of the Act is the best option to reduce the impact from scam calls and has the highest net benefit of options considered.

Consultation feedback suggests that enforceable obligations are supported by C/CSPs, individuals, government, and community organisations.

Enforceable obligations also provide more robust protections for customers through consideration of practicable and technically feasible scam disruption measures. These protections do not impose undue financial and administrative burdens on C/CSPs but significantly improve protections for the Australian community.

The status quo has large costs to consumers and businesses, posing an unacceptable level of customer harm, including from ongoing psychological distress and the potential for repeated instances of identity theft.

The education campaign may provide benefits to consumers and businesses – from providing information to help empower them to more easily identifying and managing scam calls and reducing financial losses and ongoing psychological distress. However, it does not match the benefits of placing enforceable obligations on providers to ensure consistent practices reduce the impact of scam calls. Additionally, it is noted that the enforceable obligations approach will mandate a level of consumer awareness-raising.

Effective scam call reduction at an industry-wide level will be achieved through government creating enforceable obligations on the telecommunications industry to develop improved processes and infrastructure that supports appropriate sharing of scam data, informed and proactive consumers and consistent practices.

# How will you implement and evaluate your chosen option?

## Implementation

The ACMA will register an industry code under Part 6 of the Act.

An industry code reflects industry design and ownership of the process, including engaging in public consultation and seeking agreement on technical or operational details. It encourages C/CSPs to be co-monitors of good industry-wide performance.

An industry code provides flexibility for industry to adapt to changing scammer behaviours and adjust monitoring, verifying and tracing activities accordingly to mitigate consumer detriment.

An industry code most appropriately reflects the regulatory policy intent of the Act that telecommunications be regulated in a manner that makes the greatest practical use of industry self-regulation and does not impose undue financial or administrative burdens on participants of the Australian telecommunications industry, while providing appropriate consumer safeguards.

The ACMA intends to engage with Communications Alliance to ensure C/CSPs are aware of the new enforceable obligations. This may include by providing additional guidance leading up to and following the introduction of enforceable obligations.

### Engagement with stakeholders

The direct driver for the new enforceable obligations is not industry, but third-party malicious actors. This malicious driver creates a need for ongoing flexibility for industry in adoption and delivery of adaptive scam disruption measures. Some C/CSPs have implemented (or are committed to implementing) scam call disruption measures. Their experience will be incorporated into the design of new enforceable obligations. Consultation can occur through a range of forums including the Communications Alliance working committee, STAT, and public and statutory consultation requirements.

Enforceable obligations via a registered industry code are drafted with in-built flexibility to allow C/CSPs choice in methods to implement the new obligations. This will minimise the costs of upgrading systems and support entities that have already implemented solutions from the guidance note or other initiatives to continue implementation or use of their chosen method.

Through STAT, the ACMA will work with C/CSPs and other key stakeholders where implementation issues are identified to encourage ongoing best practice in robust scam call disruption measures.

Consultation on the industry code has not indicated any issues with implementation as industry has used its own experiences to design obligations. C/CSPs will ensure staff are ready to complete the new processes at the commencement of enforceable obligations.

Customer awareness and safeguard information is expected to be straightforward to implement, with C/CSPs stating they already cover much of the information on their websites and would make updates to meet the new obligations.

An industry code registered under Part 6 includes an in-built review process. In the case of an industry code to reduce scam calls, the code will be reviewed after 2 years of the code being registered by the ACMA and every 5 years thereafter, or earlier in the event of significant developments that affect the code.

Phone scams are a compliance priority for the ACMA in 2020–21 and activities will include targeted compliance against the new obligations and potential investigations.

As an observer on the Communications Alliance working committee, the ACMA will participate in code review processes, including measuring the effectiveness of the code provisions.

The ACMA has a range of regulatory and non-regulatory tools to encourage compliance, including resources to support education and build awareness. The ACMA will leverage off its stakeholder networks to engage with industry to reduce scam calls.

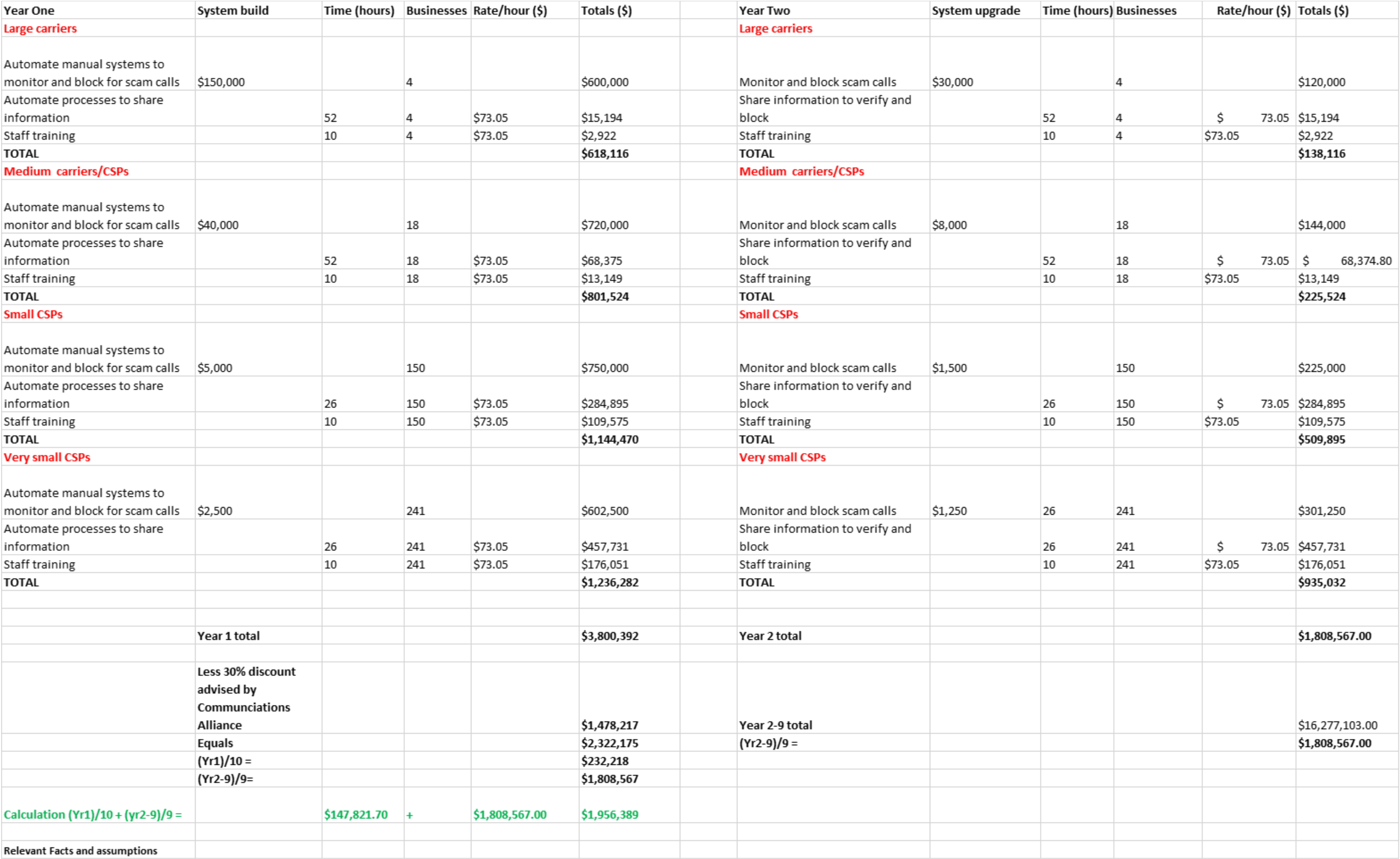
# Evaluation

The ACMA will monitor the implementation of enforceable obligations and evaluate measures through built-in review points. The enforceable obligations will also be evaluated as part of the ACMA's ongoing monitoring and compliance activities.

Phone scams are a compliance priority for the ACMA in 2020–21 and the ACMA will have an active compliance work program for the new enforceable obligations. This will include monitoring complaints about scam calls received by the TIO and escalation processes where appropriate.

Should the measures prove ineffective, the ACMA may consider regulatory reform or advice to government about implementing rules that will be fit-for-purpose to address harms and any regulatory gaps.

# Appendix A: Table 1 – Calculations to inform the regulatory burden measurement

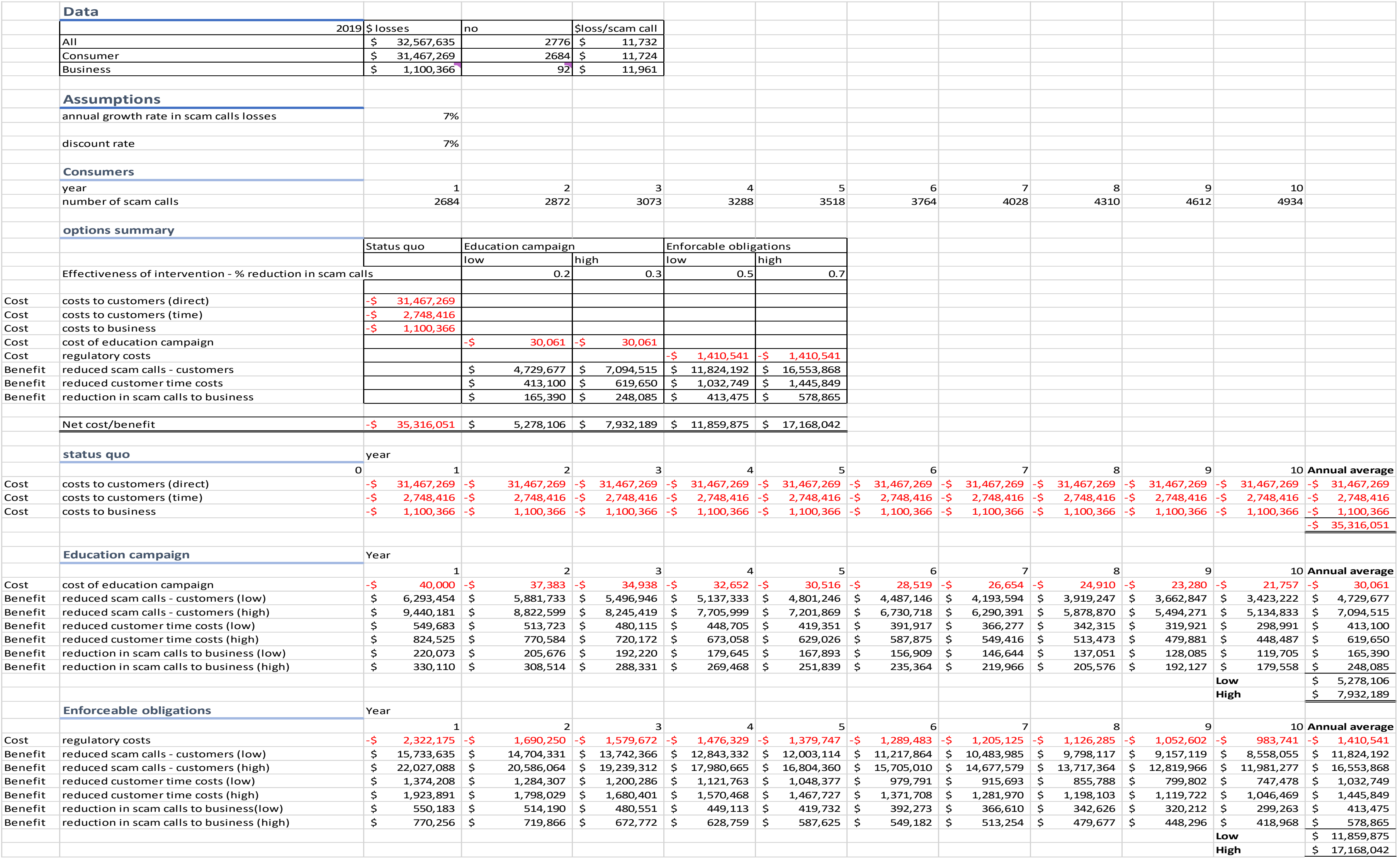


| **Year One** | **System build** | **Time (hours)** | **Businesses** | **Rate/hour ($)** | **Totals ($)** | | **Year Two** | **System upgrade** | **Time (hours)** | **Businesses** | **Rate/hour ($)** | **Totals ($)** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Large carriers** | | | | | | | **Large carriers** | | | | | |
| Automate manual systems to monitor and block for scam calls | $150,000 | | 4 | | $600,000 | | Monitor and block scam calls | $30,000 | | 4 | | $120,000 |
| Automate processes to share information | | 52 | 4 | $73.05 | $15,194 | | Share information to verify and block | | 52 | 4 | $ 73.05 | $15,194 |
| Staff training | | 10 | 4 | $73.05 | $2,922 | | Staff training | | 10 | 4 | $73.05 | $2,922 |
| **TOTAL** | | | | | **$618,116** | | **TOTAL** | | | | | **$138,116** |
| **Medium carriers/CSPs** | | | | | | | **Medium carriers/CSPs** | | | | | |
| Automate manual systems to monitor and block for scam calls | $40,000 | | 18 | | $720,000 | | Monitor and block scam calls | $8,000 | | 18 | | $144,000 |
| Automate processes to share information | | 52 | 18 | $73.05 | $68,375 | | Share information to verify and block | | 52 | 18 | $ 73.05 | $ 68,374.80 |
| Staff training | | 10 | 18 | $73.05 | $13,149 | | Staff training | | 10 | 18 | $73.05 | $13,149 |
| **TOTAL** | | | | | **$801,524** | | **TOTAL** | | | | | **$225,524** |
| **Small CSPs** | | | | | | | **Small CSPs** | | | | | |
| Automate manual systems to monitor and block for scam calls | $5,000 | | 150 | | $750,000 | | Monitor and block scam calls | $1,500 | | 150 | | $225,000 |
| Automate processes to share information | | 26 | 150 | $73.05 | $284,895 | | Share information to verify and block | | 26 | 150 | $ 73.05 | $284,895 |
| Staff training | | 10 | 150 | $73.05 | $109,575 | | Staff training | | 10 | 150 | $73.05 | $109,575 |
| **TOTAL** | | | | | **$1,144,470** | | **TOTAL** | | | | | **$509,895** |
| **Very small CSPs** | | | | | | | **Very small CSPs** | | | | | |
| Automate manual systems to monitor and block for scam calls | $2,500 | | 241 | | $602,500 | | Monitor and block scam calls | $1,250 | 26 | 241 | | $301,250 |
| Automate processes to share information | | 26 | 241 | $73.05 | $457,731 | | Share information to verify and block | | 26 | 241 | $ 73.05 | $457,731 |
| Staff training | | 10 | 241 | $73.05 | $176,051 | | Staff training | | 10 | 241 | $73.05 | $176,051 |
| **TOTAL** | | | | | **$1,236,282** | | **TOTAL** | | | | | **$935,032** |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | **Year 1 total** | | | | **$3,800,392** | | **Year 2 total** | | | | | **$1,808,567.00** |
| | | | | | | | | | | | | |
| | **Less 30% discount advised by Communciations Alliance** | | | | **$1,478,217** | | **Year 2-9 total** | | | | | $16,277,103.00 |
| | **Equals** | | | | **$2,322,175** | | (Yr2-9)/9 = | | | | | **$1,808,567.00** |
| | **(Yr1)/10 =** | | | | **$232,218** | | | | | | | |
| | **(Yr2-9)/9=** | | | | **$1,808,567** | | | | | | | |
| **Calculation (Yr1)/10 + (yr2-9)/9 =** | | **$147,821.70** | **+** | **$1,808,567.00** | **$1,956,389** | | | | | | | |
| | | | | | | | | | | | | |
| **Relevant Facts and assumptions** | | | | | | | | | | | | |

**Relevant facts and assumptions**

- 413 C/CSPs provide public number customer data for connected mobile and local services.
- C/CSPs are categorised as:
  - large carriers (>10 million services)
  - medium carriers/CSPs (1 million to 10 million services)
  - small CSPs (100,000 to 1 million services)
  - very small CSPs (<100,000 services).
- The 4 large carriers contribute 88.5% of all services; the 18 medium providers contribute 8.3% of services; the 150 small providers contribute 3% of services; and the 241 very small providers contribute 0.2% of services.
- The 4 large carriers 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 C/CSPs automate currently manual processes to monitor for scam calls and share information with other C/CSPs where scam calls are identified.
- Communications Alliance has advised the ACMA that 30% of Year 1 systems costs would have been incurred irrespective of the enforceable obligations being imposed.
- Costs in Year 2 onwards drop significantly and mainly accrue in responding to other C/CSPS identifying scam call delivered by that provider. Given the work undertaken in Year 1, it is assumed the processes will improve with staff being more experienced, and that the volume of calls requiring tracing action decreases.
- For this RIS, it is assumed that while all C/CSPs need to have processes to comply with the code, the information-sharing provisions are only enlivened when the volume of calls triggers the materiality provisions. Similarly, the requirement to share information with the ACMA and other regulators is only enlivened where a C/CSP does not respond the notifying C/CSP.
- For this RIS, it is assumed that while monitoring activities continue in real time, tracing and verifying activities (including information sharing with other providers) will occur on a weekly basis for large carriers and medium C/CSPs, and on a fortnightly basis for small and very small CSPs.

# Appendix B: Table 2 – Calculations to inform the likely annual net benefit over 10 years



**Data**

| 2019 | $ losses | no | $loss/scam call |
|---|---|---|---|
| All | $ 32,567,635 | 2776 | $ 11,732 |
| Consumer | $ 31,467,269 | 2684 | $ 11,724 |
| Business | $ 1,100,366 | 92 | $ 11,961 |

**Assumptions**

| | |
|---|---|
| annual growth rate in scam calls losses | 7% |
| discount rate | 7% |

**Consumers**

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| year | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| number of scam calls | 2684 | 2872 | 3073 | 3288 | 3518 | 3764 | 4028 | 4310 | 4612 | 4934 |

**options summary**

| | | Status quo | Education campaign | | Enforcable obligations | |
|---|---|---|---|---|---|---|
| | | | low | high | low | high |
| | Effectiveness of intervention - % reduction in scam calls | | 0.2 | 0.3 | 0.5 | 0.7 |
| Cost | costs to customers (direct) | -$ 31,467,269 | | | | |
| Cost | costs to customers (time) | -$ 2,748,416 | | | | |
| Cost | costs to business | -$ 1,100,366 | | | | |
| Cost | cost of education campaign | | -$ 30,061 | -$ 30,061 | | |
| Cost | regulatory costs | | | | -$ 1,410,541 | -$ 1,410,541 |
| Benefit | reduced scam calls - customers | | $ 4,729,677 | $ 7,094,515 | $ 11,824,192 | $ 16,553,868 |
| Benefit | reduced customer time costs | | $ 413,100 | $ 619,650 | $ 1,032,749 | $ 1,445,849 |
| Benefit | reduction in scam calls to business | | $ 165,390 | $ 248,085 | $ 413,475 | $ 578,865 |
| | Net cost/benefit | -$ 35,316,051 | $ 5,278,106 | $ 7,932,189 | $ 11,859,875 | $ 17,168,042 |

**status quo**

| | | year | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Annual average |
| Cost | costs to customers (direct) | -$ 31,467,269 | -$ 31,467,269 | -$ 31,467,269 | -$ 31,467,269 | -$ 31,467,269 | -$ 31,467,269 | -$ 31,467,269 | -$ 31,467,269 | -$ 31,467,269 | -$ 31,467,269 | -$ 31,467,269 |
| Cost | costs to customers (time) | -$ 2,748,416 | -$ 2,748,416 | -$ 2,748,416 | -$ 2,748,416 | -$ 2,748,416 | -$ 2,748,416 | -$ 2,748,416 | -$ 2,748,416 | -$ 2,748,416 | -$ 2,748,416 | -$ 2,748,416 |
| Cost | costs to business | -$ 1,100,366 | -$ 1,100,366 | -$ 1,100,366 | -$ 1,100,366 | -$ 1,100,366 | -$ 1,100,366 | -$ 1,100,366 | -$ 1,100,366 | -$ 1,100,366 | -$ 1,100,366 | -$ 1,100,366 |
| | | | | | | | | | | | | -$ 35,316,051 |

**Education campaign**

| | | Year | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Annual average |
| Cost | cost of education campaign | -$ 40,000 | -$ 37,383 | -$ 34,938 | -$ 32,652 | -$ 30,516 | -$ 28,519 | -$ 26,654 | -$ 24,910 | -$ 23,280 | -$ 21,757 | -$ 30,061 |
| Benefit | reduced scam calls - customers (low) | $ 6,293,454 | $ 5,881,733 | $ 5,496,946 | $ 5,137,333 | $ 4,801,246 | $ 4,487,146 | $ 4,193,594 | $ 3,919,247 | $ 3,662,847 | $ 3,423,222 | $ 4,729,677 |
| Benefit | reduced scam calls - customers (high) | $ 9,440,181 | $ 8,822,599 | $ 8,245,419 | $ 7,705,999 | $ 7,201,869 | $ 6,730,718 | $ 6,290,391 | $ 5,878,870 | $ 5,494,271 | $ 5,134,833 | $ 7,094,515 |
| Benefit | reduced customer time costs (low) | $ 549,683 | $ 513,723 | $ 480,115 | $ 448,705 | $ 419,351 | $ 391,917 | $ 366,277 | $ 342,315 | $ 319,921 | $ 298,991 | $ 413,100 |
| Benefit | reduced customer time costs (high) | $ 824,525 | $ 770,584 | $ 720,172 | $ 673,058 | $ 629,026 | $ 587,875 | $ 549,416 | $ 513,473 | $ 479,881 | $ 448,487 | $ 619,650 |
| Benefit | reduction in scam calls to business (low) | $ 220,073 | $ 205,676 | $ 192,220 | $ 179,645 | $ 167,893 | $ 156,909 | $ 146,644 | $ 137,051 | $ 128,085 | $ 119,705 | $ 165,390 |
| Benefit | reduction in scam calls to business (high) | $ 330,110 | $ 308,514 | $ 288,331 | $ 269,468 | $ 251,839 | $ 235,364 | $ 219,966 | $ 205,576 | $ 192,127 | $ 179,558 | $ 248,085 |
| | | | | | | | | | | | Low | $ 5,278,106 |
| | | | | | | | | | | | High | $ 7,932,189 |

**Enforceable obligations**

| | | Year | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | Annual average |
| Cost | regulatory costs | -$ 2,322,175 | -$ 1,690,250 | -$ 1,579,672 | -$ 1,476,329 | -$ 1,379,747 | -$ 1,289,483 | -$ 1,205,125 | -$ 1,126,285 | -$ 1,052,602 | -$ 983,741 | -$ 1,410,541 |
| Benefit | reduced scam calls - customers (low) | $ 15,733,635 | $ 14,704,331 | $ 13,742,366 | $ 12,843,332 | $ 12,003,114 | $ 11,217,864 | $ 10,483,985 | $ 9,798,117 | $ 9,157,119 | $ 8,558,055 | $ 11,824,192 |
| Benefit | reduced scam calls - customers (high) | $ 22,027,088 | $ 20,586,064 | $ 19,239,312 | $ 17,980,665 | $ 16,804,360 | $ 15,705,010 | $ 14,677,579 | $ 13,717,364 | $ 12,819,966 | $ 11,981,277 | $ 16,553,868 |
| Benefit | reduced customer time costs (low) | $ 1,374,208 | $ 1,284,307 | $ 1,200,286 | $ 1,121,763 | $ 1,048,377 | $ 979,791 | $ 915,693 | $ 855,788 | $ 799,802 | $ 747,478 | $ 1,032,749 |
| Benefit | reduced customer time costs (high) | $ 1,923,891 | $ 1,798,029 | $ 1,680,401 | $ 1,570,468 | $ 1,467,727 | $ 1,371,708 | $ 1,281,970 | $ 1,198,103 | $ 1,119,722 | $ 1,046,469 | $ 1,445,849 |
| Benefit | reduction in scam calls to business(low) | $ 550,183 | $ 514,190 | $ 480,551 | $ 449,113 | $ 419,732 | $ 392,273 | $ 366,610 | $ 342,626 | $ 320,212 | $ 299,263 | $ 413,475 |
| Benefit | reduction in scam calls to business (high) | $ 770,256 | $ 719,866 | $ 672,772 | $ 628,759 | $ 587,625 | $ 549,182 | $ 513,254 | $ 479,677 | $ 448,296 | $ 418,968 | $ 578,865 |
| | | | | | | | | | | | Low | $ 11,859,875 |
| | | | | | | | | | | | High | $ 17,168,042 |