Australian Government

acma

Australian Communications and Media Authority

Reducing the impact of unauthorised high-risk customer transactions

Regulation Impact Statement

FEBRUARY 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

Contents (Continued)

Introduction

The Australian Government wants to prevent unauthorised high-risk customer transactions in the telecommunications sector and mitigate fraud and associated harms to Australians.

Mobile devices often contain large amounts of personal information and 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).

However, bad actors (scammers) are increasingly finding new ways to target business processes and technologies to perpetrate scams on and through telecommunications services.

Scammers perpetrate their crimes via a range of obfuscation techniques and scam activity such as targeting weaknesses in telecommunications providers' customer authentication processes and stealing identity details or money via phone calls from live operators or robocalls.

Wide use of communications technologies as a channel to a significant range of critical transactions and social interactions has increased consumer expectations that access to those technologies and services is appropriately safeguarded from harms.

Scam activity impacts directly on the financial and emotional wellbeing of many Australians. 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.[1]

This activity also undermines confidence in our telecommunications services. There have been cases of scammers using limited personal information to access telecommunications customers' accounts and services to facilitate identity theft financial crimes.

Scams are a whole-of-community problem, and government, industry and consumers all have a role in mitigating associated detriments.

We are seeking to reduce the harm and loss caused to Australians by scammers targeting telecommunications providers' customer authentication processes where there is currently little regulatory coverage.

This will help prevent significant harms to Australian consumers and promote greater confidence in telecommunications services – regardless of which 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.

We regulate in accordance with 4 principal acts – the *Radiocommunications Act 1992*, *Telecommunications (Consumer Protection and Service Standards) Act 1999*,

[1] Identity Theft Resource Centre, 2018, *The aftermath – the non-economic impacts of identity theft*, viewed 12 October 2021.

Broadcasting Services Act 1992, and the *Telecommunications Act 1997*. We also have responsibilities under the *Interactive Gambling Act 2001,* the *Spam Act 2003* and the *Do Not Call Register Act 2006*.

Reporting and compliance

Combating scams perpetrated through telecommunications networks is a government priority, and multiple government and law enforcement agencies have statutory roles and/or receive reports of scam activity. We have a role to play as the sectoral regulator of the telecommunications industry and 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 and carriage service providers (C/CSPs).[2] They play a frontline role in protecting their customers, keeping their networks secure and in current 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 and operate international gateways that carry network traffic originating overseas and terminating in Australia.[3]

A CSP does not own network units – it provides telecommunications services over network units that a licensed carrier owns. A CSP can include organisations that resell time on a carrier network for phone calls, provide access to the internet (internet service providers) and phone services over the internet (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 the services in the commission of an offence against the Commonwealth, state, or territory.

[2] ACMA, 'About carriers and carriage service providers', viewed 5 October 2021.
[3] ibid.
[4] ibid.

What is the policy problem?

Since the first recorded attempt at fraud as far back as the year 300 BC in Greece,[5] the tactics and methods used by scammers have been constantly evolving. Yet the goal remains the same – to capture personal and financial information because it is valuable.

Scammers are criminals or bad actors who, in the telecommunications arena, often operate from offshore. They are determined and technologically agile – quickly identifying and exploiting weaknesses in systems and networks, and fraudulently gaining access to Australians' lives and finances.

While scams can be perpetrated in any number of contexts, the digital and telecommunications environments have provided attractive and generally low-cost, high-anonymity channels for scammers to use.

As COVID-19 has highlighted, more than ever, reliable communications and media services are critical to consumers, businesses, and governments. Telecommunications networks have kept Australians connected, particularly as social distancing, isolation, and quarantine arrangements disrupt usual ways of interacting. These critical networks have also been at the centre of Australia's ability to move to home-based work, telehealth, and remote schooling arrangements while continuing to support economic activity across the country.[6]

Mobile phones are an essential part of everyday life for most Australians – people use them to keep in touch with friends and family through voice calls, text messages, messaging applications and social media. Mobile phone numbers are frequently used as a means of authenticating a user for various types of accounts, including accounts with telecommunications carriers and CSPs, email and social media providers, banks and financial institutions, government, and education and retail websites. In short, telephone numbers in connection with the supply of a telecommunications service are a fundamental enabler of our digital identities.

As many consumers have their mobile phones with them at all times, text message-based 2-factor authentication can be an efficient and convenient measure to confirm a person identity prior to any number of transactions across sectors. This authentication method, however, relies upon a customer's control of their device and phone number, which is typically achieved through a SIM. Phone calls and text messages are routed to the device that has the SIM associated with the relevant phone number and service.

The use of mobile phones for 2-factor authentication means scammers target telecommunications providers' customer accounts. Scammers can 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 which uses the phone as a secondary security check.

If a scammer can receive text messages after gaining unauthorised control of a number or service, they can steal identities, obtain financial benefit, and/or fraudulently take control of Australians' digital lives.

[5] YourMoney.com, 2015, *A history of fraud through the ages and how to avoid being a victim*, viewed 16 December 2021.
[6] ACMA 2021, *Corporate plan 2021–22*, viewed 8 October 2021.

Scammers perpetrate 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.[7]

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 next section).

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.[8]

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 a key enabler of 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.[9]

In addition to facilitating the commission of other offences, organised crime groups may also sell stolen identity information to other criminal networks. When a person has their identity stolen, they may experience repeated victimisation. In this way, organised crime groups can use fraudulent identities to cause considerable additional financial loss.

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.[10]

[7] Commonwealth Fraud Prevention Centre, (counterfraud.gov.au), viewed 5 October 2021.
[8] Identity crime and misuse in Australia (homeaffairs.gov.au), viewed 10 October 2021.
[9] Attorney-General's Department, '*Fraud in Australia*', viewed 10 October 2021.
[10] Australian Institute of Criminology, 2020, *Identity crime and misuse in Australia 2019*, viewed 11 October 2021.

Impact of identity crime on victims

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.[11]

The true impact remains unknown as losses are almost certainly under-reported because many are embarrassed by falling victim to scams.

Scamwatch is the primary government website used by Australians to report scams, and it is estimated only around 13% of all victims of scams will make a report to Scamwatch.[12]

Victims may report their experiences in many ways – from discussing what occurred with family and friends, through to reporting to consumer protection agencies, businesses, and/or reporting to police and other government regulators.

Identity crime continues to affect a large number of Australians, as well as businesses and government agencies. Victims of fraud also suffer very real emotional distress and trauma. These impacts can be severe and long-term as people try to recover what is often, and increasingly, an integral part of their digital identities.

Victims may report to one or all of the government or consumer agencies that take reports – such as the ACMA, ACCC, Telecommunications Industry Ombudsman (TIO), IDCARE[13] and the Australian Cyber Security Centre (ACSC).[14] 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.[15]

Australians who are the victim of identity theft typically suffer both financial loss and psychological harms. As seen in the table below, the consequences can include experiencing reputational damage and health problems to experiencing mental and emotional distress. The effects can be life-altering, impacting health, emotional wellbeing and relationships with others.[16]

[11] ACCC, 2021, *Targeting scams 2020*, viewed 11 October 2021.
[12] ibid.
[13] 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.
[14] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 13 October 2021.
[15] Australian Institute of Criminology, 2019, 'Identity crime and misuse in Australia', viewed 10 October 2021.
[16] Identity Theft Resource Centre, 2018, *The aftermath – the non-economic impacts of identity theft*, viewed 12 October 2021.

Source: AIC 2020, Identity crime and misuse in Australia 2019.

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.[17]

AIC also found that victims required 34 hours on average to deal with the consequences of their personal information being misused[18] while IDCARE estimated that an average of 32 hours is spent by customers to address identity theft.[19] These figures do not include lost productivity, where a customer has taken time off work to address identity theft.[20]

Identity theft has long-term repercussions for victims as victims can also experience multiple instances of fraud over months or years and IDCARE recommends victims set up yearly reporting to allow for continual monitoring.[21]

Some of the impacts are also captured in the 3 case studies in this document. These examples draw on reports from victims of identity theft and fraud to highlight not only the financial impacts but also the psychological and emotional harms to Australians from unauthorised actions performed on their accounts.

Case study 1: Jen's Twitter takeover

When Jen's* small business Twitter account was taken over by hackers, a stream of tweets with profanities and slurs were posted for an hour. Jen was the victim of a SIM swap scam, where scammers took control of her business mobile phone account through a mixture of obfuscation techniques and online stalking.

Jen's business suffered reputational damage that has been hard to reverse, in addition to $25,000 in lost earnings as customers cancelled orders believing Jen was behind the offensive tweets.

[17] IDCARE unpublished data supplied to Australian Institute of Criminology for *Identity crime and misuse in Australia*, 2019, viewed 20 October 2021.
[18] Australian Institute of Criminology, 2020, *Identity crime and misuse in Australia 2019*, viewed 11 October 2021.
[19] IDCARE 2018, 'Unauthorised Mobile Phone Porting Events', IDCARE Insights bulletin.
[20] ibid.
[21] Australian Institute of Criminology, 2019, *Identity crime and misuse in Australia*, viewed 9 October 2021.

Jen later found out that the scammers had obtained her personal details by mining data stolen during the breach of a different company's systems, and then contacted her mobile phone provider pretending to be her to request the SIM swap.

Fraudsters will often use information that has been put up on social media, like mother's maiden name or pet names, and use this information to build up a profile of information on a potential victim. Unfortunately for Jen, her active social media presence had inadvertently made her particularly vulnerable.

Jen spent months trying to resolve the damage to both her personal reputation as well as her business brand. She has had to invest in new businesses systems and upgrade her data protection measures. Jen has spent hours with the social media companies to re-establish her accounts and is still trying to rebuild her customer base.

**Case study is based on one or more reports of SIM swap fraud to a government agency. Names of individuals and companies have been changed.*

Incidence of scams in Australia

Research commissioned by the ACCC in 2019 shows that Scamwatch is just one of many places people report scams, and only a third of people who respond to a scam go on to report that scam to a government agency.[22]

In 2020, Scamwatch obtained data from other government agencies,[23] 8 banks and 2 remittance service providers to better illustrate the harm caused by scams – with reports of $851 million in combined losses from scams.[24]

- Scamwatch received the largest number of reports – with $176 million reported lost – an increase of around 23% from the $143 million in losses reported in 2019.
- Of these reports, almost 21,000 reports of identity theft were received – representing an increase of 84% from 2019.[25]

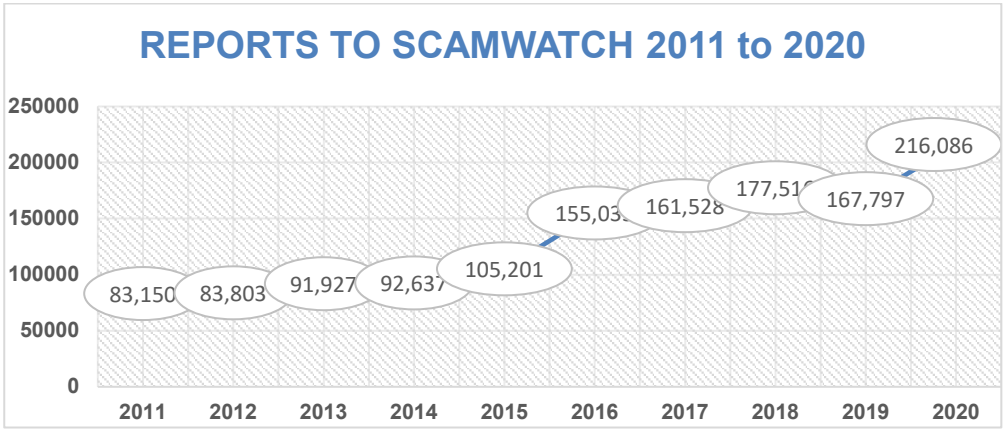
Between 1 January and 19 September 2021, Australians have reported a record $211 million in losses to scams to Scamwatch – an 89% increase from the same period in 2020 – with the reported losses surpassing the $176 million reported to Scamwatch across all of 2020.[26]

Data from Scamwatch indicates that reported losses from identity theft are continuing to rise – in late 2021 (1 Jan to 30 September 2021), it had received reports of $7,754,647 in financial losses to identity theft – an increase of 234% on 2020.[27]

While the increase could be partially attributed to more Australians turning to an online environment because of COVID-19 lockdowns, and scammers similarly adapting, the table below indicates that reports of scam activity have been increasing over the 10 years since 2011.[28]

[22] ACCC, 2021, *Targeting scams 2020*, viewed 20 October 2021.
[23] Government agencies included data received from ReportCyber, the Australian Taxation Office, Services Australia, the Australian Securities and Investments Commission , WA ScamNet and the ACMA.
[24] ACCC, 2021, *Targeting scams 2020*, viewed 20 October 2021.
[25] ibid.
[26] ACCC Scamwatch media release, 2021, *Losses reported to Scamwatch exceed $211 million, phone scams exploding*, viewed 18 October 2021.
[27] These losses came from 1,012 reports across all methods – 4.0% reports with financial losses, ACCC Scamwatch online statistics 1 January to 30 September 2021, viewed 11 October 2021.
[28] ACCC Scamwatch Scam statistics, viewed 24 October 2021.

Scammers are agile, sophisticated, and quick to respond to emerging technologies to take advantage of changing environments.



Source: ACCC Scamwatch 2021.

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 create more opportunity for identity crime and fraud.

Scam activity on telecommunications networks

Most indicators are that scam activity on Australian telecommunications networks is at a significant, historically high level. It is increasingly sophisticated and hard to detect. It generally originates offshore, readily adapts to disruption measures and ruthlessly exploits new opportunities and vulnerabilities.

Often scammers' methods involve the fraudulent collection of personal information and data to commit identity fraud. For example, scammers may make direct phone calls from live operators or robocalls or send a barrage of text messages with links to fraudulent websites. Scammers will ask the individual to 'prove' who they are or ask for access to their device or computer to direct a victim towards downloading software that allows a scammer to take control of personal accounts.

Scammers will also make false promises or look to incentivise individuals to act on something – such as opportunities to buy products, invest money, receive free product trials or a prize or grant, or references to unpaid tax or a computer virus. Some may even threaten legal action or financial loss to push the victim to act.

Scammers 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 – such as quickly exploiting the transition to an online environment and government support packages for Australians during the COVID-19 pandemic.

Scamwatch reports – phone-based scams

In 2020, reports of scams by phone or text accounted for 62.7% of all reports to Scamwatch:

- $51.3 million in losses from phone or text – a 43.9% increase in losses from 2019 ($35.63 million losses)
- 135,490 reports from phone or text – up 39% in 2020 from 2019 (97,416 reports).

Many of the losses reported to Scamwatch in 2021 were from phone-based scams, which to the end of September accounted for over $63.6 million (31%) of the $211 million reported losses. Additionally, of the 213,000 reports that Scamwatch received to the end of September, 113,000 were about phone scams.[29]

The reported losses to phone-based scams in the 12-month period to September 2021 is evidence that the trend is continuing. As table 1 shows, there have been 220,714 reports and over $90,842,325 million in losses. This is a 77% increase in financial losses on the year before and an 62.9% increase in reported scams to Scamwatch.

Table 1: Scamwatch 12-month combined reports of scams via phone and text[30]

12 months to September 2021	Monetary loss	Reported w/ financial loss (F/L)	Number of scams reported	Average loss	Average loss of reporting F/L
All reports	$90,842,325	8.6%	220,714	$412	$4,786

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

High-risk customer transactions

Anyone can fall prey to a scam as a result of a high-risk customer interaction regardless of age, gender, education or economic background.

A high-risk customer interaction is any interaction that could, where unauthorised access is gained, result in a customer losing access to their telecommunications service or theft of their personal information.

It may include where a customer has contacted a CSP or where a CSP contacts a customer, and the CSP discloses customer information or makes a change to the telecommunications service provided to a customer or their account. For example, to enable a SIM swap[31] request, call diversion request, post-paid to pre-paid mobile service request, or any request to change information in customer accounts (such as change of address or adding an authorised account holder).

Scammers target CSPs' authentication processes to gather sufficient information to later pose as the customer to facilitate a transaction, such as a fraudulent SIM swap or 'purchasing' expensive handsets and allowing scammers to gain full access to customer accounts and payment details. This includes making phishing[32] calls to

[29] ACCC Scamwatch media release, 2021, *Losses reported to Scamwatch exceed $211 million, phone scams exploding*, viewed 18 October 2021.
[30] ACCC Scamwatch scam statistics, viewed 26 October 2021.
[31] Subscriber identity module (SIM) swaps can legitimately occur when a consumer has lost their phone or SIM or is transferring the number connected to a mobile service to a new device that requires a different size SIM. This does not involve a change of provider. Unauthorised SIM swap occurs when a customer's number is transferred to a new SIM in a new device that is in the control of a scammer.
[32] Phishing is a way that cybercriminals steal confidential information, such as online banking logins, credit card details, business login credentials or passwords/passphrases, by sending fraudulent messages (sometimes called 'lures'). These deceptive messages often pretend to be from a large organisation you

CSPs' customer service representatives to harvest the details they need or to make changes to the target's account.

Current customer authentication measures

There are no specific regulatory obligations on C/CSPs in relation to high-risk customer transactions; however, they have an obligation under Part 13 of the Telecommunications Act to protect the confidentiality of information relating to communications carried or supplied. C/CSPs also have an obligation under Part 14 of the Telecommunications 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.

C/CSPs have obligations to protect personal information under the *Privacy Act 1988* (the Privacy Act) as well as under Part 6 of the Telecommunications Act. C/CSPs also view the relationship with their customers as commercially sensitive and want to protect their customer base.

There are obligations on providers to check a customer's identity before buying or activating a prepaid mobile service set out in the Telecommunications (Service Provider – Identity Checks for Prepaid Mobile Carriage Services) Determination 2017.

There are also ACMA-registered enforceable industry codes developed by Communications Alliance Ltd[33] that specify technical and operational requirements, including the Telecommunications Consumer Protections Code, and Mobile Number Portability Code. These codes include key commitments to protecting consumers' privacy and obligations when obtaining a customer's consent and authorisation prior to porting a service to another provider.

The arrangements for customer authorisation are contained in the Customer Authorisation Industry Guideline. The guideline streamlines and simplifies information provided to and gathered from customers when transferring a service. It sets out:

- common information to be provided to all customers before they agree to transfer their number
- information to be obtained from the customer to obtain a valid customer authorisation.

Compliance with an industry guidance note is not mandatory nor enforceable by the ACMA.

Multi-factor authentication

Multi-factor identity verification, often referred to as '2-factor authentication', offers an effective security control to prevent malicious actors from gaining access to a device, and any sensitive information within. Two-factor identification identifies a user by utilising something the person knows (like a password or code sent to them) and something they have (their mobile phone). When implemented correctly, it can be a highly effective strategy to mitigate harm, particularly where remote authentication is required.

In 2020, we introduced the Telecommunications (Mobile Pre-Porting Additional Identity Verification) Industry Standard 2020 (the PPV Standard) to address the harms caused by mobile porting fraud. It sets out additional identity verification processes that

trust to make the scam more believable. They can be sent via email, SMS, instant messaging, or social media platforms. They often contain a link to a fake website where you are encouraged to enter confidential details.

[33] Communications Alliance Ltd (Communications Alliance) is Australia's peak communications industry body. Membership is drawn from a cross-section of the communications industry, including service providers, vendors, consultants, and suppliers.

gaining mobile CSPs must complete prior to initiating a port of a customer's number – including the use of multi-factor customer identity verification processes.

There is strong evidence that the implementation of the PPV Standard has led to a significant drop in unauthorised mobile porting.[34] Major telecommunications providers have reported an approximate drop of 95% in reported porting fraud cases.[35] The Australian Competition and Consumer Commission (ACCC)[36] also released figures showing an approximate 50% reduction in reported losses from mobile number porting in 2020 following the commencement of the PPV Standard in April 2020.[37]

However, the protections in the enforceable obligations set out in the PPV Standard do not extend to other types of high-risk customer transactions, such as SIM swap requests or requests to change customer account information. These requests rely on customer authentication processes that differ from provider to provider and how a customer contacts each provider or the channel they use (e.g., online, phone or in-store). These business processes can be exploited – and that gap allows scammers to target customer accounts to commit fraud and identity crime.

Case study 2: Simon's SIM swap

Simon* was recently the victim of SIM swap fraud, where his number was transferred by his phone provider to a new pre-purchased eSIM[38] which had been issued to an unauthorised person following a phone call by the scammer to his provider.

The unauthorised person was identified by providing Simon's name, date of birth and phone number. On the basis of that information, the unauthorised person was able to request that an eSIM be issued and sent to an email address that did not belong to Simon and was not registered to his account with his provider.

Simon's provider advised that the caller was sufficiently identified by name, date of birth and mobile and therefore they had met their obligations to confirm identity under the current rules. No further steps were taken to verify that the caller was Simon, and no email or SMS was sent by his provider prior to the swap completion to verify that the request was genuine.

As a result of this, Simon suffered a substantial financial loss of $15,000, and loss of identity documents which were stored in his online drive. The psychological impact on Simon was also significant, with the knowledge and anxiety that his identity could potentially be used to defraud other innocent victims.

**Case study is based on one or more reports of SIM swap fraud made to a government agency. Names of individuals and companies have been changed.*

Scammers targeting weak customer authentication processes

Australian consumers are experiencing significant harm perpetrated by scammers targeting weaknesses in telecommunications providers' customer authentication processes where there is currently little regulatory coverage. This involves

[34] Mobile number portability allows customers to change telecommunications providers without changing their mobile phone number. It is a fast and effective competition measure for mobile carriage service providers and their customers, Mobile porting fraud occurs where, upon request by a scammer, a customer's number is ported from their current mobile carriage service provider to another in the control of the scammer, generally enabled by use of false or stolen identification.
[35] Unpublished confidential data as reported to the ACMA from Australian C/CSPs.
[36] 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.
[37] ACCC, 2021, *Targeting scams 2020*, viewed 11 October 2021.
[38] eSim: An embedded-SIM, or embedded universal integrated circuit card, is a form of programmable SIM that is embedded directly into a device.

unauthorised actions performed on customer accounts as well as a lack of protection of consumer's personal information from unauthorised access.

For example, when a mobile phone owner loses, breaks, or upgrades their mobile phone, they can sometimes take the SIM card out of their previous mobile phone and insert it into their new phone. Often, however, the customer needs to contact their CSP, explain that they are changing devices, and request that their CSP reassign the account information to the SIM in their new device. When a scammer successfully impersonates the customer and convinces the CSP to change the real customer's mobile phone service to a new SIM in a device that the scammer controls, the scammer gains access to all of the information associated with the customer's account, and gains control over the customer's phone number and receives both the customer's text messages and phone calls.

Once an unauthorised SIM swap request has been completed, the scammer has acquired the potential means to take over many more of the victim's accounts. Such account takeover tactics can cause substantial consumer detriment.

As a further example, text messages are often used by banks, businesses, and payment services to verify a customer's identity, when a customer requests updates to those accounts. Intercepting a text message used to authenticate a customer can allow a scammer to reset a customer's password and take over the customer's financial, social media, and other accounts. Having taken over these accounts, the scammer can then change the login details, drain bank accounts, steal cryptocurrency, and sell or try to ransom social media accounts.[39] Loss of service on a customer's device – the phone going dark or only allowing emergency calls – is typically the first sign of unauthorised SIM swapping for a customer.

Reported fraud

Data from key stakeholders indicates ongoing and emerging harms from scammers targeting customer authentication processes. It is difficult to quantify due to the various reporting options, underreporting and types of fraud.

We have received data from other government agencies, CSPs and other bodies, including entities in the financial sector, for the period 1 January to 30 September 2021 that provides strong evidence of ongoing, realised harm. In particular, that scammers are targeting SIM swap processes,[40] with some data sources indicating harms have in fact increased. The data does not holistically cover attempted or unrealised reported fraud to CSPs or to a range of banks or financial institutions.

It is also acknowledged that scam attempts from unauthorised customer transactions and their impacts are likely to be much higher as Scamwatch research – and ACMA data matching – has found that scams are grossly under-reported to government.[41]

Between 1 January and 30 September 2021, we are aware of at least 510 incidents of reported fraud with $4,680,665.22 in financial losses. From these, 163 reported a financial loss for an average loss of $28,715.74 per incident – with the largest single reported financial loss being $463,782.[42]

It is important to note that these reports and losses continue despite some CSPs already implementing scam disruption and enhanced identity authentication measures.

[39]ACSC 2021, *ACSC - Small and medium businesses*, viewed 22 October 2021.
[40] Unpublished ACMA analysis indicates that between January and May 2021, more than 80% of mobile number fraud resulted from unauthorised SIM swap.
[41] ACCC Scamwatch, 2021, *Targeting scams 2020*, viewed 20 October 2021.
[42] ACMA analysed several datasets from specific entities, agencies and bodies that rely on consumer reports. The dataset may overlap or be captured in different ways (including the period involved) by the bodies that collect it, e.g., some financial entities combining porting fraud and SIM swap fraud into the same category.

While technology to combat scams evolves, so does scammers use of new obfuscation techniques and methods.

Case study 3: Lucien loses out

Lucien received an SMS from his provider at 11:30 pm saying his registered contact details had been changed and to contact his provider as soon as possible if he had not made these changes. Lucien immediately tried to call his provider to report he had not made the changes. Because he called after business hours, he received a recorded message asking him to call back after 9:00 am the next day.

When Lucien called his provider the next morning, the provider confirmed Lucien's registered email address had been changed and agreed to restore the original email address. Because of Lucien's concerns about his account security, his provider placed a password on the account and said Lucien would need to quote the password whenever he wanted to make changes to his account.

One hour later, Lucien's mobile phone lost service and he found the passwords for his email address, internet banking account and myGov account had all been changed.

It was discovered that the provider had not asked the scammer to provide Lucien's password on second and subsequent access attempts. It had instead authenticated the scammer by asking for Lucien's address and account number.

The scammer was able to provide this information and process a SIM swap, giving them access to Lucien's mobile number. They then used their access to the mobile number to complete 2-factor authentication and reset the passwords on Lucien's other accounts.

Case study from the TIO submission to the Communications Alliance consultation on an industry code 2021.

International experience

Australia is not alone in grappling with the problem of scammers targeting weaknesses in telecommunications providers' customer authentication processes. Other jurisdictions are looking at a range of measures to address high-risk customer transactions such as unauthorised SIM swap and porting requests.

New Zealand (NZ)

In NZ, mobile number porting is regulated under the *Telecommunications Act 2001* and administered by the Commerce Commission and the NZ Telecommunications Forum (TCF). In June 2021, the TCF introduced new rules for consumers (who switch mobile providers and want to keep their phone number) to receive a dedicated SMS text message to help prevent fraudsters.[43] The dedicated SMS is part of a series of measures the mobile phone industry in NZ is implementing to make it much tougher for scammers to exploit the number porting system.

A more advanced SMS solution is also under development in NZ. Once implemented, customers who have had a porting request on their account will receive an SMS from

[43] TCF, 2021, *Mobile phone providers introduce new security measures to prevent Number Porting fraud*, viewed 5 November 2021.

their current provider to which they will need to reply 'YES' in order for the number porting process to occur.[44]

NZ mobile providers have also tightened up the requirements for customers to verify their identification when requesting a SIM swap. Providers that have physical stores now require these customers to present their identification in-store.[45]

United Kingdom (UK)

Ofcom is the UK regulator of communications services – including broadband, home phone and mobile services. It collaborates with industry, police, government, and other regulators to ensure strong actions are in place to tackle the threat posed by scam text and calls. Ofcom also supports industry's work to develop technical solutions and engages in consumer awareness campaigns of the steps people can take to protect themselves.[46]

In July 2019, Ofcom introduced a new way to handle number portability for UK customers – establishing a 'text-to-switch'[47] process that allows people to switch mobile provider by sending a simple, free text message to their current provider (texting 'PAC' to the number 65075 allows a porting request to occur).

Ofcom also encourages anyone who receives a suspicious text message to report it by forwarding the message to '7726', which directs the message to the relevant mobile provider. The numbers can then be investigated and potentially blocked if found to be a persistently rogue number – helping to disrupt scam activity and prevent more people being exposed to scam attempts.

UK mobile phone companies have been criticised after allowing the details of customers to be disclosed. An investigation in 2020 by consumer group Which?[48] into reports of SIM swap fraud found that despite safeguards, there had been a 400% increase over 5 years. Criminals were able to subvert the rules and get the information they need through persistence.[49]

Recent research released by Ofcom also shows that in the summer of 2021, almost 45 million people received potential scam texts or calls in the UK.[50] More than 8 in 10 (82%) said they had received a suspicious message, in the form of either a text, recorded message or live phone call to a landline or mobile.[51]

Ofcom remains concerned about the significant rise in scam calls and texts over the last 18 months as the tactics used by scammers are becoming increasingly sophisticated – including using multiple communication channels and impersonating the brands of well-known companies and organisations. It continues to work with providers and law enforcement to tackle scams.[52]

United States (US)

In 2019, the Federal Bureau of Investigation (FBI) warned of the risks of SIM-swapping. The FBI wanted more complex forms of authentication to be introduced

[44] ibid.
[45] ibid.
[46] Ofcom, 2021, Ofcom website, viewed 5 November 2021.
[47] The provider replies by text within a minute and sends a switching code, called a 'PAC', which will be valid for 30 days. Their reply must also include important information – such as any charges that have to be paid if leaving a contract early, or any credit balance if a pre-paid customer. The PAC is provided to the new provider, who must arrange for the switch to be completed within one working day.
[48] Which?, 2020, *SIM swap fraud - How criminals hijack your number to get into your bank accounts*, viewed 3 November 2021.
[49] ibid.
[50] Ofcom, 2021, *45 million people targeted by scam calls and texts this summer*, viewed 4 November 2021.
[51] ibid.
[52] ibid.

after seeing an increase in the use of SIM swapping by criminals to steal digital currency using information found on social media – including personally identifying information or details about the victim's digital currency accounts.[53]

The Federal Communications Commission (FCC) is an independent government agency overseen by Congress that is the primary authority for communications law, regulation, and technological innovation. On 30 September 2021, the FCC began 'a formal rulemaking process with the goal of confronting subscriber identity module (SIM) swapping scams and port-out fraud – both of which bad actors use to steal consumers' cell phone accounts without ever gaining physical control of a consumer's phone'.[54]

The FCC had received numerous complaints from consumers who have suffered significant distress, inconvenience and financial harm because of SIM swapping and port-out fraud. In addition, recent data breaches exposed customer information that could potentially make it easier to pull off these kinds of attacks.

The FCC has recently consulted on a proposal to amend the Customer Proprietary Network Information (CPNI) and local number portability rules to require carriers to adopt secure methods of authenticating a customer before redirecting a customer's phone number to a new device or carrier. It also proposed requiring providers to immediately notify customers whenever a SIM change or port request is made on customers' accounts.[55] New rules are anticipated in 2022.

[53] FBI, 2019, *FBI San Francisco Warns the Public of the Dangers of SIM Swapping*, viewed 3 November 2021.
[54] FCC, 2021, *FCC Proposes Rules to Prevent SIM Swapping and Port-Out Fraud*, viewed 3 November 2021.
[55] ibid.

2. Why is government action needed?

Government priority

International and local experience indicates that there is no single or simple solution to preventing fraud and combating phone scams. Technological solutions to scam disruption need to sit within a broader framework to be effective, which is why 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.[56]

In November 2019, the then Minister for Communications, Cyber Safety and the Arts endorsed the project's 3-point 'Combating scams' action plan – including forming a joint government-industry taskforce (STAT),[57] developing new enforceable obligations and immediately trialling new scam reduction initiatives.

In April 2020, the government introduced new measures to prevent mobile porting fraud[58] that included setting out verification processes to confirm that the person initiating the port holds the rights of use to that number. The new measures have seen a reduction in reports of mobile porting fraud of approximately 95%.[59]

In December 2020, we followed this by registering new rules requiring C/CSPs to detect, trace and block scam calls. In the first 7 months of the new rules being in force, industry blocked over 214 million scam calls.[60] While these scam mitigation measures have significantly reduced the impact of mobile porting fraud and are promising in relation to reducing scam calls received by Australians, they do not address the impact and harms associated with high-risk customer transactions.

The government's policy objective is to reduce the incidence of fraud and identity crime from scams occurring, given the realised harms and potential for Australians to experience significant impacts.[61] Government wants to work with regulators, law enforcement agencies and industry to keep Australians safe from harm. At present, there are no current enforceable obligations concerning high-risk customer transactions in Australia, and fraud prevention activities are inconsistent across the telecommunications industry.

Communications Alliance has recently developed an industry code (C666:2021 Existing Customer Authentication)[62] and submitted it to us for potential registration. The proposed code seeks to provide a common set of principles for CSPs to use to

[56] 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.
[57] 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.
[58] Mobile porting fraud is used by malicious third-party actors to 'hijack' a person's mobile phone and gain access to their bank accounts and other applications containing sensitive information or are capable of receiving personal information, such as unique verification codes.
[59] Unpublished confidential data as reported to the ACMA from major CSPs.
[60] Minister Fletcher media release, *Over 200 million scam calls blocked*, viewed 10 October 2021.
[61] Minister Fletcher 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 4 November 2021.
[62] Communications Alliance, 2021, Industry code C666:2021, viewed 12 November 2021.

put authentication procedures in place. It is supported by a confidential guidance note[63] that would be available to Communications Alliance members to support implementation of the industry code. The guidance note is intentionally non-public to avoid alerting those that seek to commit fraud of the detailed actions being taken to safeguard against them. The government was not involved in drafting the guidance note.

We note that breaches of an industry code require it to direct a company to comply with the code and identify further non-compliance before it can access the full range of its stronger enforcement powers.

While CSP-led scam-disruption initiatives are welcomed, they also raise further questions about how protections will be afforded to all customers – as not all CSPs have acted to adopt measures to protect customer accounts, while some have implemented better security provisions than others. This gap in protections creates further opportunities for scammers to target customer accounts, which has consequences for all Australians.

Action is required now

Without government action, Australian telecommunications users are at risk of scammers taking control of phone accounts and significantly impacting on people's financial and digital lives without ever gaining physical control of a consumer's phone.

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 2-step verification 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 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.

The problem of scams increasing despite concerted efforts by government, law enforcement and industry to limit scams perpetrated on telecommunications networks. As previously noted, Scamwatch research shows that scams are both under and inconsistently reported – victims may report to none, one or all the government or consumer agencies that take reports, leading government to underestimate the scale of the problem.

Any gap in efforts by government and industry to prevent fraud and address the problem of unauthorised high-risk customer transactions will be exploited by scammers. It is an ongoing challenge, because once a solution is found to address one type of scam, the scammers involved target new weaknesses. By way of example, if a consumer has a fixed and mobile service with a provider, and regulatory obligations do not attach to transactions for both, it is likely that scammers will target the 'unprotected' channel.

[63] The confidential guidance note was initially developed by Communications Alliance in 2019 and sits behind a member paywall. It is not published due to concerns about how scammers might use the information.

Improving the consumer safeguards requirements for customer authentication across all service types (via enhanced identity verification processes covering all points at high risk of fraud in customer transactions) can significantly reduce the number of Australians impacted by the harms associated with unauthorised transactions.

Government action that compels a consistent approach to community-wide customer protection measures provides the strongest approach to achieving an outcome for the Australian community.

3. What policy options have been considered?

The policy options below are consistent with regulatory options available in accordance with the Telecommunications Act to meet the government's objectives of reducing the incidence of fraud and identity crime from scams occurring, given the significant potential for Australians to experience harms.

Option 1: Non-regulatory option (status quo)

The government continues to encourage the telecommunications industry to implement voluntary customer authentication measures and provides general advice to consumers on avoiding fraud, identity theft and scams (for example, through Scamwatch, ReportCyber and ACMA resources setting out how consumers can protect themselves). The existing legislation and regulations for CSPs remain – including obligations under Part 13 and Part 14 of the Telecommunications Act.

Communications Alliance encourages CSPs to act in accordance with industry guidance, with members deciding whether to voluntarily comply. Those providers deploying measures continue to use them in addition to existing laws and regulations to help reduce instances of fraud.

Under this option, CSPs would continue with the disparate (and mainly larger CSP level) operational approaches currently employed to manage customer authentication fraud.

No compliance requirements or enforcement options would apply. Scams will still occur, and it is likely the volume of calls and harms escalate as no industry-wide technological nor network strategies have been implemented to reduce unauthorised high-risk customer transactions.

Australians will continue to experience significant harms as there will be varying levels of protection from scammers – while scammers will continue to exploit, and target, weak links, and ineffective authentication processes.

Option 2: Consumer education campaign

The government does not introduce any new form of regulation but instead conducts a targeted public education campaign that builds on existing phone scams resources to provide clear and accessible information to assist consumers to better manage and avoid fraud over telecommunications networks. The existing legislation and regulations governing CSPs remain.

The campaign focuses on advising customers how to improve their online and physical identity for phone and customer account security – and what to do if they become a victim of a fraudulent customer authentication interaction – including where to report it.

Information is provided to 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 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 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 consumers who may be in vulnerable circumstances (such as some older Australians and First Nations Australians) to inform and help them better manage scam calls. However, some members of the community may not receive nor understand the information.

The campaign is run annually for 10 years by the ACMA in accordance with usual practice and builds on our other campaigns. A campaign based upon the below steps will cost on average $30,560 per annum (depending on the size of the intended audience):

- information published on ACMA and other government websites
- a short 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 and First Nations Australians audience
- targeted ads on social media to reach consumers
- use of LinkedIn to reach business, consumer groups and C/CSPs
- use of direct email lists
- promotional materials with key messages (such as magnets, notepads, pens)
- boosting impressions of the social media content (potentially reaching over 7.7 million people).

This option relies entirely on better informed Australians reacting appropriately to the campaign. Industry behaviour may still present potential or realised harms as the majority of engagement with CSPs will be for the purposes of education and compliance with the existing regulatory framework.

Option 3: Enforceable obligations

The government introduces new regulation in the form of enforceable obligations that require CSPs to better protect customer accounts when where there is a high risk of scammers targeting the transactions to perpetrate identity and/or financial theft.

This includes establishing robust industry-wide and consistent measures for all CSPs that have regulatory parity with the PPV Standard to address the serious nature of the harms involved. The obligations will prevent particular channels being targeted by scammers if protections are, or are perceived to be, weaker than other channels.

Enforceable obligations strongly align with the government's objective of reducing the incidence of fraud and identity crime from scams occurring. A CSP would be required to adopt enhanced identity verification processes to prevent harm to existing customers arising from unauthorised high-risk customer transactions.

A CSP would be obliged to take measures designed to help prevent identity theft and associated financial losses occurring through unauthorised transactions. This would include not proceeding with a high-risk customer interaction unless the customer's identity is verified by robust processes – i.e., multi-factor identity verification processes have been used.

A CSP would also be required to provide customers with additional levels of protection if requested by the customer (such as instances where their identity documentation has been compromised and/or subject to past theft).

The stronger protection measures are also designed to ensure that genuine customers – particularly those who are vulnerable, disadvantaged or in an emergency situation – can still undertake transactions with their service provider.

This option proposes enforceable obligations be principle or outcomes-based (to the extent they can) to avoid providing sensitive information to scammers. The enforceable obligations would permit adaptive and flexible initiatives to address scams and/or do not stifle potential innovation.

Depending on the mechanism chosen to deliver enforceable obligations, we can act under Part 4 or Part 6 of the Telecommunications Act to ensure CSPs comply with requirements that will help reduce harms to Australian telecommunications users.

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

If the status quo is maintained, the Australian community will continue to be subject to fraudulent transactions as scammers can target any Australian with a telecommunications account.

Benefits

CSPs that have not implemented stronger customer authentication processes may benefit from choosing not to implement any additional processes beyond what is currently deployed or required to meet existing obligations under Parts 13 and 14 of the Telecommunications Act, although it is noted that such a provider may be subject to reputational loss and lack of consumer confidence.

Costs

It can be anticipated that the impact of harms associated with unauthorised high-risk customer transactions 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, a conservative average annual increase of 25% has been applied to measure the growing consumer detriment. This considers the trend of increasing reports and associated losses reported to Scamwatch in the 12 months to September 2021.[64]

It can be anticipated that if the status quo remained, reported losses for Australians will continue to increase, and there would be, on average, at least $13.5 million in financial losses each year over a 10-year period due to fraud from unauthorised high-risk customer transactions.[65]

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

Assuming each customer notifies their financial institution, the financial cost of fraud may be borne by those institutions – with customers potentially able to recover money lost through fraud protection policies. However, it is not clear all frauds are reported or

[64] This considers that from 2019 to 2020, Scamwatch received an increase of 23% in all scam reports on 2019 – with combined losses from phone and text up 19.88%, while losses from identity theft increased by 84%. While for the 12-month period to September 2021, data from Scamwatch indicates that reports are continuing to rise. Additionally in the 12 months to September 2021, scam reports vis phone and text increased by 63% and financial losses by 77%.[64]

[65] See Appendix B of this RIS for calculations.

that recompense occurs in all cases, while the costs borne by financial institutions are likely to increase insurance costs and/or be recovered across the customer base.

In addition, while many 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.[66]

The impact on individuals whose identity is stolen goes beyond economic losses suffered. Identity theft affects more than just any single individual. The fraud can also impact those close to victims, with financial and psychological stress involved.[67] In some extreme cases, victims have difficulties in finding employment, are refused services, or are refused credit due to the fraud.[68]

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, contact government services that might be compromised (such as myGov, ATO, Medicare), their financial institutions (banks, superannuation, investment firms) and their CSP.

For the purposes of the RIS, it is assumed that it takes on average 33 hours for victims to address identity theft. This represents a minimum cost of $1,056 per victim – or total losses of $718,080 per year.[69] This represents, on average, an annual total cost of $1,549,920 in time each year over a 10-year period.[70]

CSPs

This option does not generally impose any additional regulatory costs on CSPs.

Option 2: Consumer education campaign

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 protecting their identity.

Benefits

In 2019, Scamwatch heard from 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.[71] A consumer education campaign would broadly target all Australians to become better informed about how to protect their personal information. It would help reduce the impact of harms (albeit only to the extent this personal information is used in frauds targeting high risk customer processes) incurred by Australians as a consequence of weak customer authentication measures.

Australians will be engaged in an education campaign which provides tools and resources that can help empower them to respond when responding to a CSP or engaging in a high-risk customer interaction – for example, by taking control of how they share their personal information in public and guidance on what to do if they are a victim of identity theft or fraud.

[66] Identity Theft Resource Centre, 2018, *The aftermath – the non-economic impacts of identity theft*, viewed 19 October 2021.
[67] ibid.
[68] Australian Institute of Criminology, 2019, *Identity crime and misuse in Australia*, viewed 19 October 2021.
[69] Calculated at the OBPR leisure labour rate of $32 per hour for private citizens and based on an estimate of 680 reports for 12 months in 2021.
[70] Compound growth over 10 years discounted at 7% each year (see Appendix B of this RIS).
[71] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 16 October 2020.

Over time, there has been a shift from reports of scams seeking money to reports about scams seeking information.[72] An informed individual is more likely to better protect their personal information and may increase reports, which will help reduce the harms associated with scam over telecommunications networks.

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 CSPs what they are doing to prevent misuse of their personal information before choosing a service provider.

This may incentivise CSPs to voluntarily increase identity protections in accordance with the status quo, which may also reduce instances of fraud and identity crime. It is assumed better informed consumers will drive more CSPs to view voluntary additional protections as aligned to their existing regulatory 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 CSP that voluntarily implements stronger customer authentication measures may help stop thousands of Australians being targeted by scammers.

An educational campaign may have reputational benefits for the telecommunications industry – particularly for CSPs that can demonstrate their commitment to improved protections for their customers as CSPs that adopt good practices may have a competitive advantage by being able to advertise themselves as a trusted provider that protects the identity of their customers.

Initial benefits

The practical impact of an education campaign could result in an estimated 10 to 20% reduction in the impact of fraud compared to the status quo. This reduction is due to the increase in CSPs adopting voluntary protections and the impact of better informed and proactive customers.

Yet, 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 an equivalent decrease of up to 20% in instances of psychological harm caused by identity theft from fraudulent customer transactions, and the need for consumers to seek support services.

The initial benefits[73] of this reduction represent prevention of financial losses to fraud from high-risk transactions of between $1,013,517 and $2,027,034 each year comprising of:

- direct savings of $908,934 to $1,817,869
- savings in time spent by customers responding to identity theft of between $104,582 to $209,165[74]
- freeing up of financial institution and/or telecommunications fraud team[75] resources by 10 to 20% 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 10 to 20%).

[72] ACCC, 2020, *Targeting scams 2019: A review of scam activity since 2009*, viewed 16 October 2020.
[73] See Appendix B of this RIS.
[74] Figure based on reduced reports of all high-risk incidents at a rate of $32/hour for 33 hours, averaged and discounted over 10 years.
[75] Equivalent to 10 to 20% of C/CSP fraud team time.

Costs

Better informed customers may increase workloads for fraud teams – as Australians will be more responsive to the signs of scams. Financial institutions and CSPs will continue to need to spend time and resources responding to fraud and identity theft from unauthorised high-risk customer transactions, as well as assisting customers to manage the impact.

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

Option 3: Enforceable obligations

Benefits

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

Enforceable obligations have the potential to provide significant positive impacts by reducing the financial and emotional harms that an individual may face from fraudulent activity.

Mandating better identity protection would also be consistent with the government's National Identity Security Strategy and National Identity Proofing Guidelines.[76] Placing enforceable obligations on CSPs to protect customers through enhanced authentication processes will also provide improved opportunities for referral for regulatory or law enforcement action.

The most significant benefit from enforceable obligations will be a reduction in the financial impact on Australians. For this assessment, it is conservatively estimated that enforceable obligations will result in a 70% reduction in the impact of scams and fraud from unauthorised high-risk customer transactions – depending on the mechanism used to set obligations. This will also leverage the existing regulatory framework – including system and process changes to implement the PPV Standard.

CSPs

Enforceable obligations provide the opportunity to enforce and promote consistent, industry-wide approaches to combating scams by establishing processes and protections that provide certainty for CSPs and their customers.

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

The benefits[77] of this option represent:

- average annual savings from financial losses to fraud of approximately $7,094,617
- direct savings to consumers of around $6,362,540[78]

[76] Department of Home Affairs 2016, National Identity Proofing Guidelines, viewed 11 October 2021. The guidelines provide guidance about the preservation and protection of a person's identity as a 'key concern and a right of all Australians'.
[77] Compound growth fraud and time costs over 10 years discounted at 7% each year (see Appendix B).
[78] Based on a 70% reduction in $3.1 million of direct losses to consumers in the status quo.

- annual savings in time spent by customers responding to identity theft of approximately $732,077[79]
- a 70% decrease in instances of psychological harm caused by identity theft resulting from unauthorised access to customer accounts and details, and the need for consumers to seek support services
- freeing up of financial institution or telecommunications fraud team resources to assist customers on other matters (equivalent to savings of 70%)
- a reduction in the resources required by support organisations to assist customers who have experienced identity theft relating to unauthorised high risk transaction fraud (equivalent to savings of 70%).

A mandatory approach to addressing customer authentication processes provides a reputational benefit for CSPs. It demonstrates to consumers that CSPs are regulated and have industry-wide measures that will improve consumer safeguards and disrupt fraudulent activity.

It provides positive benefits for CSPs 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, CSPs – which are relentlessly targeted by scammers impersonating their brands and attempting to steal the identity of their customers – benefit from the extra protections.

Costs

There are no direct costs to Australian customers from enforceable obligations; however, the Australian community can expect to benefit from collaborative and coordinated action to address unauthorised high-risk customer transactions over telecommunications networks.

Experience has shown there is no ‘silver bullet’ to addressing scams. Scammers are able to quickly pivot to take advantage of changing environments – as seen most recently with the coronavirus pandemic.

Costs to the community come from the residual instances of fraudulent transactions that is, those not reduced by the enforceable obligations, including from the impact of psychological harm and distress experienced by each victim of a fraudulent interaction and the ongoing repercussions of identity theft.

CSPs

Ensuring enforceable obligations are outcomes-based, to the extent possible, will provide flexibility for CSPs in complying. For example, it may be more efficient for providers to automate their systems, but for a smaller carriage service provider with less customers, the necessary activities could be conducted manually. Providers may also choose which type of multi-factor identification they use, including for specific channels.

Each CSP is responsible for exactly determining how they monitor their network to detect and act against fraudulent customer transactions and it is anticipated that 70% of costs for systems automation would have accrued to comply with existing obligations.

[79] Figure based on reduction reports * 33 hours * $32 discounted over 10 years.

Where costs accrue under enforceable obligations, costs will be higher for CSPs who have failed to implement multi-factor authentication processes prior to obligations coming into force.

The number of CSPs that will be covered by enforceable obligations has been conservatively estimated at a maximum of 412. This maximum includes each CSP; however, there are a number of partnerships and carrier relationships in place. For example, some smaller CSPs are owned by larger CSPs, while others purchase network capacity to provide services to their customers.

It is anticipated that while all CSPs will need to have processes to comply with new enforceable obligations, CSPs already incur ongoing costs associated with complying with the obligations in the PPV Standard and can leverage off those measures.

It is estimated on average that the total annual regulatory costs would be $765,391 over 10 years.[80]

As Table 2 shows below, costs from Year 2 drop significantly and mainly reflect the activity involved in responding to new business process developments.

Table 2: Costs to all CSPs to comply with enforceable obligations over 10 years[81]

Category	Costs: Year 1	Cost: Year 2 onwards
Large	$453,285	$92,190
Medium	$739,724	$157,149
Small	$914,363	$334,575
Very small	$866,576	$477,301
Sub-total	$2,973,948	$1,061,215
Discounting sunk costs	$2,081,764	
Total	**$892,184**	**$1,061,215**

Given the work undertaken in Year 1, it is assumed the processes will improve with staff being more experienced, and that the volume of fraudulent authentication requiring 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 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 stronger authentication measures may potentially divert scammers to other markets or services (such as apps and social networking sites). These other platforms are also the subject of government action. For example, the ACCC is conducting the Digital Platform Services Inquiry to consider whether there is a need for regulatory reform to address the competition and consumer concerns identified in digital platform services markets to date. [82] In addition, the ACSC has

[80] See Appendix A of this RIS for a breakdown of regulatory costs.
[81] See Appendix A of this RIS for a further breakdown of costs.
[82] ACCC, Digital platform services inquiry 2020-2025, viewed 14 October 2021.

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 unauthorised high-risk customer transactions through enforceable obligations will make Australia a harder target for scammers overall and have specific benefits such as restoring confidence in the telecommunications networks that underpin the way Australians engage in the modern world. It must be a coordinated approach, or the weakest link will be targeted.

Regulatory burden measurement table

Option	Regulatory cost (annual)
Status quo	n/a
Consumer education campaign	n/a
Enforceable obligations	$765,391

We anticipate that the regulatory burden for all CSPs to comply with enforceable obligations is around $0.77 million annually for 10 years.

This assumes that:

- 70% of costs for systems automation would have accrued to comply with existing obligations already introduced
- costs will be higher for the 3 CSPs that are also 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	0.1	0.2	0.7
Cost	Costs (direct)	$13,470,470	$13,470,470	$13,470,470	$13,470,470
Cost	Costs (time)	$1,549,920	$1,549,920	$1,549,920	$1,549,920
Cost	Education campaign cost		$22,528	$22,528	
Cost	Regulatory costs				$765,391
Benefit	Reduced fraud		$908,934	$1,817,869	$6,362,540
Benefit	Reduced time costs		$104,582	$209,165	$732,077
Net cost/benefit		**-$15,020,390**	**-$14,029,401**	**-$13,015,884**	**-$8,691,163**
Total benefits			**$1,013,517**	**$2,027,034**	**$7,094,617**

** Assumes 25% annual growth in fraudulent transactions, 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 CSPs that will incur regulatory costs.*

Who was consulted and what did they say?

Consultation

Since 2019, we have been working closely with the ACCC, ACSC and other government agencies and departments to disrupt scams targeting Australians. We have also worked with Communications Alliance (and its members through the Scam Telecommunications Action Taskforce or STAT) to explore ways to reduce scam activity over telecommunications networks.

We established the STAT in early 2020 as a key action from the *Combating scams* action plan to build cross-government and industry collaboration on scams across telecommunications services. Key participants include the ACCC, the ACSC, telecommunications providers, the finance sector, police, the Australian Tax Office, Services Australia, and Australia Post.

The STAT operates on the principle that reducing harms to Australian telecommunications users can only be achieved through working together to develop processes and infrastructure that support a consistent, industry-wide approach to combating scams. The taskforce meets 3 times per year where the current threat environment, and existing and emerging disruption initiatives, are discussed.

Significant stakeholder engagement and consultation has also occurred around developing enforceable obligations to reduce the impact of scams on telecommunications services.[83] We introduced requirements on industry to prevent mobile porting fraud (PPV Standard) and registered an industry code to reduce scams calls (C661:2020 Reducing Scam Calls).[84]

Given the evolving targets and techniques used by scammers, the STAT (and its associated working groups) have provided a forum to identify emerging issues and share approaches to combat scams or participate in scam reduction initiatives. This has included monitoring the issue of unauthorised high-risk customer transactions. We have regularly engaged with industry to better understand the problem and options to ensure community-wide protections are in place.

We also convene the Numbering Advisory Committee (NAC) approximately 2 to 3 times a year to assist us in performing its functions relating to management of Australia's numbering resources. Members of the NAC include representatives from consumer organisations, CSPs, industry associations and government representatives.

In 2021, the NAC discussed the need for measures to reduce fraudulent customer transactions, including:

- the development of digital authentication measures
- the then in-development customer authentication industry guideline
- whether stronger measures (like enforceable obligations) were required to monitor CSPs actions in reducing fraud resulting from unauthorised high-risk customer transactions.

[83] ACMA 2020, RIS Mobile porting fraud, RIS Reducing the Impact of Scam Calls, viewed 12 November 2021.
[84] Communications Alliance 2020, (C661:2020) Reducing Scam Calls, viewed 12 November 2021.

We have regularly sought data to understand the magnitude of the issue and information about any actions taken by CSPs to address the negative impact of unauthorised high-risk customer transactions on Australians. Industry advice indicated that while PPV Standard processes has been successful in reducing incidences of mobile porting fraud, the obligations are not designed to address other customer identity verification processes including SIM swap requests, updating billing and customer account information.

CSPs are supportive of new enforceable obligations, noting the exact form of such regulations is not settled or agreed, as it affects their customer base. Discussions with the 3 major carriers that operate as CSPs have also revealed that to varying degrees, each have implemented (or are implementing), a range of measures to try to prevent fraud from unauthorised high-risk customer transactions. These include strengthening multi-factor authentication controls for high-risk customer account transactions and increasing protections around access to SIMs.

Those that have implemented enhanced protections in relation to all or some customer transactions have advised us that strengthening multifactor authentication controls around high-risk customer account transactions has proven an effective measure. It is viewed as a potential way to not only reduce SIM swap fraud but also other current (and emerging types) of fraud attempted by scammers.

We have also corresponded with CSPs about additional better practice approaches that some mobile CSPs had adopted to further protect customers from mobile porting fraud and their applicability to existing customer authentication practices. These approaches included unique verification code messages being sent to customers, providers flagging ‘at risk’ accounts, and notifying customers about port-out requests. Providers have generally supported these business improvements to improve customer protections.

We have similarly engaged with the Australian Financial Crimes Exchange (AFCX), IDCARE and the Australian Communications Consumer Action Network (ACCAN) to understand their view of the problem. All recognise the significant impact on Australians and are supportive of further measures being introduced. We have also been keeping the Department of Infrastructure, Transport, Regional Development and Communications (DITRDC), ACCC and TIO informed of our findings.

The ACMA recently formed an industry reference group to further improve understanding of existing industry practices, including having regard to customer identity verification processes that CSPs have implemented or are in the process of implementing (including those set out in the draft industry code).

There is general agreement from most stakeholders that government and industry must act to reduce the significant harms being experienced by Australians because of unauthorised high-risk customer transactions. Where stakeholder views differ on the problem, is in the mechanism that should be used to introduce enforceable obligations. Generally, government and consumer groups support direct regulation to mitigate the significant harms faced by Australians while industry favours a co-regulatory approach.

Consultation on enforceable obligations

In September 2021, Communications Alliance demonstrated support for enforceable obligations by releasing a draft code – C666:2021 Existing Customer Authentication Industry Code – for public comment. Submissions closed in October 2021, and the code was recently submitted to the ACMA for registration.

Four submissions were received in response to the draft code,[85] and all 4 supported the introduction of measures that improved customer authentication to prevent harms. Some of the key themes raised in those submissions included:

- clarification of the objectives and scope of the code
- clarification of the definition for high-risk transactions and whether a list of high-risk interaction types would be beneficial
- the option of CSPs including self-service options for high-risk transactions
- implementation issues of biometric data or possession-based authentication methods
- considering only disclosing call detail or account information via customer-initiated contact.

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 us to substantiate that appropriate consultation was undertaken with the ACCC, OAIC and the TIO.

As per section 117 of the Telecommunications Act, we must also consult with the OAIC that it is satisfied with such a code – particularly if it deals with matters under the Privacy Act.

While an industry code is one of the regulatory options available to us to introduce enforceable obligations, we have explored some of the issues raised prior to and post-consultation on the industry code. Our priority is to implement the most effective solution to address the considerable consumer detriment being experienced.

On 17 November 2021, we commenced a public consultation process on a draft service provider determination to gather further input and test assumptions. The process included:

- publication of a consultation paper and draft instrument (via our website)
- targeted consultation with government agencies and consumer groups
- consultation with the reference group, STAT, Communications Alliance, and other industry stakeholders
- consultation with other organisations including those that support victims of identity crime and those that support family violence and emergency-affected people.

The consultation closed on 16 December 2021. We received 14 submissions during the process from consumer and industry representatives and other government organisations. Key themes from the submissions include:

- Implementation timeframe – industry members argue that the commencement date proposed in the draft determination obligations will be difficult to meet while other stakeholders would like to see more immediate measures.
- Definition of high-risk transactions – different CSPs have varying views on how the definition may impact in the draft determination and what limits it may place on customer transactions. Industry argues that the determination is overly prescriptive. Industry also argues that many of the transactions that will be captured are not high-risk (for example, they argue that there is no evidence that scammers are targeting business transactions) and that such an approach will have a material

[85]Communications Alliance, 2021, Public comments, viewed 5 November 2021. Communications Alliance received 4 submissions – from ACCAN, TIO, Twilio (CSP) and RingCentral (a provider of business integrated communications and collaboration solutions over the cloud).

burden on carriers (and customers) noting that multiple systems and processes that will need to be updated. Industry instead suggests that CSPs should retain some discretion around what constitutes a high-risk interaction.

- Definition of ‘vulnerable customers’ – both consumer groups and telcos say that the definition is too narrow and not consistent with the outcome we are trying to achieve. Further, there is the view that the carve-out (section 11) provides a handbook for scammers on how to exploit the carve-out.
- Customer verification requirements – industry argues that the customer verification requirements (drawn from the PPV) are not suitable for all transactions captured by the determination and, in any case, are too prescriptive, and CSPs should maintain discretion on how to achieve the required outcomes, using existing systems and processes where feasible.

The matters raised via the consultation process have benefited from further follow-up engagement and testing with key stakeholders to inform future decisions about the preferred implementation approach to the recommended option.

What is the best option from those considered?

Scammers are technologically adept, increasingly sophisticated and show no signs of stopping. Australians are at risk from the impact of considerable harms. This emphasises the need for government to encourage practical technological solutions that increase the effectiveness of preventing and disrupting scam call activity on Australian telecommunications networks.

Consultation and engagement to date clearly indicates that enforceable obligations are supported by CSPs, individuals, government, and community organisations, because they best address the serious nature of the harms involved.

The Australian community can expect to benefit greatly from government introducing enforceable obligations that mandate action to address fraudulent customer transactions and provide increased consumer safeguards. It has the highest net benefit of the options considered.

Enforceable obligations have the potential to provide significant positive impacts by reducing the financial and emotional harms that an individual may face from fraudulent activity. Enforceable obligations will also offer better identity protection, consistent with the government's guidance on robust identity verification.[86]

These protections do not impose undue financial and administrative burdens on CSPs but significantly improve consumer protections for the Australian community and confidence in industry's networks and services as key conduits to participation in the modern economy and, for many, social life. Considering the telecommunications industry has already absorbed costs to implement processes and systems to meet their obligations under the PPV Standard, aligning new enforceable obligations to protect high-risk customer transactions will cause less financial cost and administrative burden than it may have otherwise.

In developing the enforceable obligations, we will consider the existing customer authentication processes that most providers have already implemented or are in the process of implementing as per the current industry guidance note and draft code. The measures outlined in the draft code demonstrate industry's general support of enforceable obligations to mitigate the significant impacts associated with this issue.

Status quo (non-regulatory option)

The status quo poses an unacceptable level of harm to Australians. The community will continue to experience increasing levels of identity theft and financial losses as a result of unauthorised high-risk customer transactions, because no consistent nor 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 may provide some benefits to the community to support a reduction in financial losses, and ongoing psychological distress – from providing

[86] Department of Home Affairs 2016, National Identity Proofing Guidelines, viewed 11 October 2021.

information that encourages Australians to be more aware of protecting their digital identity to CSPs more effectively protecting customers' accounts.

However, it does not match the benefits of placing enforceable obligations on providers to ensure consistent practices are in place to reduce the significant impact of identity theft and fraud because of unauthorised high-risk customer transactions. Additionally, it is noted that the enforceable obligations approach will mandate a level of consumer awareness-raising that also supports enhanced identity verification processes and consistent, industry-wide practices.

How will you implement your chosen option?

Implementation

We may develop a service provider determination under subsection 99(1) of the Telecommunications Act to implement enforceable obligations on the basis that (as required by Regulation 10 of the Telecommunications Regulations 2021) it would relate to the interest that customers of service providers have in relation to the supply of specified carriage services.

The determination would also provide us with a wide range of immediately available enforcement options such as:

- formal warning
- enforceable undertaking
- remedial directions
- infringement notice (for infringement notices to be available the provisions must be listed in the Telecommunications (Listed Infringement Notice Provisions) Declaration 2011)
- commencement of proceedings in the Federal Court of Australia.

We may also determine an industry standard under Part 6 of the Telecommunications Act in limited circumstances:

- where it has requested an industry body[87] to make an industry code and they have not (section 123)
- if there is no industry body or association formed (section 124)
- or an industry code that has been made is deficient (section 125).

We must determine an industry standard if directed by the Minister in accordance with section 125AA of the Telecommunications Act. Industry standards apply to participants in a particular section of the telecommunications industry; and may deal with one or more matters relating to the telecommunications activities of those participants.

Alternatively, we may register a code submitted by industry under Part 6 of the Telecommunications Act. As noted on page 33, a precursor to code registration is that we must be satisfied that Communications Alliance has consulted as per section 117 of the Telecommunications Act. We must also consult with the OAIC that it is satisfied with the code – particularly if it deals with matters under the Privacy Act.

Our enforcement options in the event of a code breach are formal warning or direction to comply with a code. Once an entity is directed to comply with a code, enforcement actions include pursuing civil penalties through the Federal Court or an infringement notice issued if a direction to comply is then breached (under Part 31 of the Telecommunications Act).

[87] An industry code is drafted by a representative industry body (such as Communications Alliance) and registered by the ACMA as per section 117 of the Telecommunications Act.

Engagement to support implementation

We intend to engage with Communications Alliance to ensure CSPs are aware and understand the introduction of new enforceable obligations. This may include by providing additional guidance leading up to and following their introduction.

Engagement can also occur through a range of forums including the Communications Alliance working committee, STAT, and NAC. Discussion in these forums will be enable us to stay informed of, and potentially address, any implementation concerns that industry may have and encourage ongoing best practice.

The direct driver for the new enforceable obligations is not industry, but scammers. This malicious driver creates a need for ongoing flexibility for industry in adoption and delivery of adaptive scam disruption measures. To the extent possible, the enforceable obligations will be drafted with in-built flexibility to allow CSPs a degree of choice in how to implement the new obligations.

Phone scams are a compliance priority[88] for us in 2021–22 and activities will include targeted compliance against the new obligations and potential investigations. This will include monitoring complaints received by the TIO, ACCC, ACSC and the financial sector and risk-based escalation interventions where appropriate.

We will work with industry so that industry is aware it must comply with new obligations at the time they come into effect. We are aware that some CSPs have been proactive in implementing multifactor identity verification processes to address fraud from unauthorised high-risk customer transactions. We are also aware that CSPs are at different stages of implementation, which is also reflected in the level of fraud they are experiencing. Smaller providers may have minimal processes in place to meet the proposed new rules.

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

Education campaign

We have a range of regulatory and non-regulatory tools to encourage compliance, including resources to support education and build awareness. We will leverage off our stakeholder networks to engage with industry to reduce the detriment caused to consumers by fraud from unauthorised high-risk customer transactions.

While an education campaign did not have the greatest net benefit as a standalone option to address this issue, a modest, targeted education program may be used to help customers and industry transition. Such a program will need to be circumspect on any technical detail to avoid scammers using the information to find ways to bypass additional customer identity verification processes.

[88] ACMA, 2021, ACMA Compliance priorities 2021–22, viewed 11 October 2021.

Evaluation

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

As previously discussed, phone scams are a compliance priority for the ACMA in 2021–22 and, given the harms involved, are likely to be a key focus in forward years.

The ACMA will have an active compliance work program for the new enforceable obligations. This will include monitoring complaints about identity theft and fraud resulting from unauthorised high-risk customer transactions received by the TIO, the financial sector and government agencies and escalation processes where appropriate. It will also include reviewing reports received by the ACCC, AFCX and ACSC.

Additionally, the STAT will provide a regular forum to monitor and evaluate the effectiveness and success of the measures set out in the enforceable obligations, as will research into the consumer experience conducted by us on a regular basis.

Success will be measured by the ACMA seeing a notable reduction in the reports of unauthorised high-risk customer transactions, research findings and a decrease in the associated harms from incidences of fraud and identity theft from scams perpetrated over telecommunications networks.

Should the measures prove ineffective, we 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 2	System upgrade	Time (hours)	Businesses	Rate/hour ($)	Totals ($)
Large Carriers						**Large Carriers**					
Automate manual systems to enhance processes	$150,000		3		$ 450,000	Monitor processes	$30,000		3		$ 90,000
Staff training		15	3	$73	$ 3,285	Staff training – ongoing		10	3	$73	$ 2,190
Total					**$ 453,285**	**Total**					**$ 92,190**
Medium CSPs						**Medium CSPs**					
Automate manual systems to enhance processes	$40,000		18		$ 720,000	Monitor processes	$8,000		18		$ 144,000
Staff training		15	18	$73	$ 19,724	Staff training		10	18	$73	$ 13,149
Total					**$ 739,724**	**Total**					**$ 157,149**
Small CSPs						**Small CSPs**					
Automate manual systems to enhance processes	$5,000		150		$ 750,000	Monitor processes	$1,500		150		$ 225,000
Staff training		15	150	$73	$ 164,363	Staff training		10	150	$73	$ 109,575
Total					**$ 914,363**	**Total**					**$ 334,575**
Very small CSPs						**Very small CSPs**					
Automate manual systems to enhance processes	$2,500		241		$ 602,500	Monitor processes	$1,250		241		$ 301,250
Staff training		15	241	$73	$ 264,076	Staff training		10	241	$73	$ 176,051
Total					**$ 866,576**	**Total**					**$ 477,301**
	Year 1				**$ 2,973,948**	**Year 2 total**					**$ 1,061,215**
	Discounted cost				**$ 892,184**						

Relevant facts and assumptions

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

- 412 CSPs provide public number customer data for connected mobile and local services:
  - large carriers (also CSPs): 3 (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 3 large carriers contribute approximately over 90% of all services and 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 CSPs reflect consistent systems and training processes.
- We anticipate that 70% of Year 1 systems costs would have been incurred irrespective of enforceable obligations being imposed.
- Costs in Year 2 onwards drop significantly and mainly accrue in responding to new processes. Given the work undertaken in Year 1, it is assumed the processes will improve with staff being more experienced, and that the volume of fraudulent customer transactions requiring action decreases.

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

See below spreadsheet.

Data

	Monetary Loss	Reported w/ Financial Lo	Number of Scams Reporte	Average Loss	Average Loss of Reporting F/L
High risk incidents (Jan - Sep 2021)	$ 4,680,665	32.0%	510	$ 9,178	$ 28,681
All reports (Sep 2020 - Sep 2021)	$ 90,842,325	8.6%	220714	$ 412	$ 4,786

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	$30,560
High risk incidents with F/L in Year 1	218
High risk incidents (all) in Year 1	680
Regulatory Costs - Year 1 (discounting for sunk co	$892,184
Regulatory Costs - Year 2 onwards	$1,061,215

Consumers

Year	1	2	3	4	5	6	7	8	9	10
All high-risk scam incidents	680	850	1063	1328	1660	2075	2594	3242	4053	5066
High-risk scam incidents with F/L	218	272	340	425	531	664	830	1038	1297	1621

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	$ 13,470,470	$ 13,470,470	$ 13,470,470	$ 13,470,470	$ 13,470,470	$ 13,470,470	$ 13,470,470
Cost	Time Cost of Scam Activity	$ 1,549,920	$ 1,549,920	$ 1,549,920	$ 1,549,920	$ 1,549,920	$ 1,549,920	$ 1,549,920
Cost	Regulatory Cost	$ -	$ -	$ -	$ -	$ 765,391	$ 765,391	$ 765,391
Cost	Education Campaign Cost	$ -	$ 22,528	$ 22,528	$ 22,528	$ -	$ -	$ -
Benefi	Reduced Fraud	$ -	$ 908,934	$ 1,363,401	$ 1,817,869	$ 5,453,606	$ 6,362,540	$ 7,271,474
Benefi	Reduced Time Costs	$ -	$ 104,582	$ 156,874	$ 209,165	$ 627,495	$ 732,077	$ 836,660
	Net Cost Benefit	-$ 15,020,390	-$ 14,029,401	-$ 13,522,643	-$ 13,015,884	-$ 9,704,680	-$ 8,691,163	-$ 7,677,646
	Benefit from Reduction in Scam Fraud	$ -	$ 1,013,517	$ 1,520,275	$ 2,027,034	$ 6,081,101	$ 7,094,617	$ 8,108,134

Option 1: Status Quo

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Direct Costs of Scam Activity	$ 6,240,887	$ 7,255,031	$ 8,433,973	$ 9,804,494	$ 11,397,724	$ 13,249,854	$ 15,402,956	$ 17,905,936	$ 20,815,651	$ 24,198,194	$ 13,470,470
Cost	Time Cost of Scam Activity	$ 718,080	$ 834,768	$ 970,418	$ 1,128,111	$ 1,311,429	$ 1,524,536	$ 1,772,273	$ 2,060,267	$ 2,395,061	$ 2,784,258	$ 1,549,920

Option 2: Education Campaign

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Cost of Education Campaign	$ 30,560	$ 28,421	$ 26,431	$ 24,581	$ 22,860	$ 21,260	$ 19,772	$ 18,388	$ 17,101	$ 15,904	$ 22,528
Benefi	Reduced Fraud	$ 936,133	$ 1,012,077	$ 1,094,182	$ 1,182,947	$ 1,278,914	$ 1,382,665	$ 1,494,834	$ 1,616,103	$ 1,747,209	$ 1,888,951	$ 1,363,401
Benefi	Reduced Time Costs	$ 107,712	$ 116,450	$ 125,897	$ 136,111	$ 147,153	$ 159,090	$ 171,996	$ 185,950	$ 201,035	$ 217,344	$ 156,874

Option 3: Enforceable Obligations

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Regulatory Costs	$ 892,184	$ 986,930	$ 917,845	$ 853,596	$ 793,844	$ 738,275	$ 686,596	$ 638,534	$ 593,837	$ 552,268	$ 765,391
Benefi	Reduced Fraud	$ 4,368,621	$ 4,723,025	$ 5,106,180	$ 5,520,419	$ 5,968,263	$ 6,452,439	$ 6,975,893	$ 7,541,812	$ 8,153,642	$ 8,815,106	$ 6,362,540
Benefi	Reduced Time Costs	$ 502,656	$ 543,434	$ 587,520	$ 635,183	$ 686,712	$ 742,421	$ 802,650	$ 867,765	$ 938,163	$ 1,014,271	$ 732,077

Option 2: Education Campaign (Low)

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Cost of Education Campaign	$ 30,560	$ 28,421	$ 26,431	$ 24,581	$ 22,860	$ 21,260	$ 19,772	$ 18,388	$ 17,101	$ 15,904	$ 22,528
Benefi	Reduced Fraud	$ 624,089	$ 674,718	$ 729,454	$ 788,631	$ 852,609	$ 921,777	$ 996,556	$ 1,077,402	$ 1,164,806	$ 1,259,301	$ 908,934
Benefi	Reduced Time Costs	$ 71,808	$ 77,633	$ 83,931	$ 90,740	$ 98,102	$ 106,060	$ 114,664	$ 123,966	$ 134,023	$ 144,896	$ 104,582

Option 2: Education Campaign (High)

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Cost of Education Campaign	$ 30,560	$ 28,421	$ 26,431	$ 24,581	$ 22,860	$ 21,260	$ 19,772	$ 18,388	$ 17,101	$ 15,904	$ 22,528
Benefi	Reduced Fraud	$ 1,248,177	$ 1,349,436	$ 1,458,909	$ 1,577,263	$ 1,705,218	$ 1,843,554	$ 1,993,112	$ 2,154,803	$ 2,329,612	$ 2,518,602	$ 1,817,869
Benefi	Reduced Time Costs	$ 143,616	$ 155,267	$ 167,863	$ 181,481	$ 196,203	$ 212,120	$ 229,329	$ 247,933	$ 268,046	$ 289,792	$ 209,165

Option 3: Enforceable Obligations (Low)

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Regulatory Costs	$ 892,184.00	$ 986,930	$ 917,845	$ 853,596	$ 793,844	$ 738,275	$ 686,596	$ 638,534	$ 593,837	$ 552,268	$ 765,391
Benefi	Reduced Fraud	$ 3,744,532	$ 4,048,307	$ 4,376,726	$ 4,731,788	$ 5,115,654	$ 5,530,662	$ 5,979,337	$ 6,464,410	$ 6,988,836	$ 7,555,805	$ 5,453,606
Benefi	Reduced Time Costs	$ 430,848	$ 465,801	$ 503,589	$ 544,442	$ 588,610	$ 636,361	$ 687,986	$ 743,799	$ 804,139	$ 869,375	$ 627,495

Option 3: Enforceable Obligations (High)

Year		1	2	3	4	5	6	7	8	9	10	Annual Average
Cost	Regulatory Costs	$ 892,184.00	$ 986,930	$ 917,845	$ 853,596	$ 793,844	$ 738,275	$ 686,596	$ 638,534	$ 593,837	$ 552,268	$ 765,391
Benefi	Reduced Fraud	$ 4,992,709	$ 5,397,743	$ 5,835,635	$ 6,309,051	$ 6,820,872	$ 7,374,216	$ 7,972,449	$ 8,619,214	$ 9,318,448	$ 10,074,407	$ 7,271,474
Benefi	Reduced Time Costs	$ 574,464	$ 621,067	$ 671,451	$ 725,923	$ 784,813	$ 848,481	$ 917,315	$ 991,732	$ 1,072,186	$ 1,159,167	$ 836,660