Australian Government

acma

Australian Communications and Media Authority

Mobile porting fraud—Regulation Impact Statement

FEBRUARY 2020

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 minimise fraudulent mobile number porting and reduce associated financial loss and hardship to consumers.

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.

An ever-increasing number of adults now use a mobile service (and fewer have a home landline).[1] Mobile devices often contain large amounts of personal information and are regularly used for security verification for a range of utilities and accounts, including government services such as the myGov portal to access government services online.

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

There have been cases of scammers using specific personal information obtained from online or other sources (such as mailbox theft) to fraudulently port a person's mobile number from their current service provider to another. Scammers have then used the ported number to access the consumer's bank accounts and authorise transactions by sending bank verification codes to the number.

Scammers are finding new ways to target Australian mobile phone customers.[2] They are technologically adept, increasingly sophisticated and show no signs of stopping.

The Australian Communications and Media Authority (the ACMA) is seeking to prevent the harm and loss to customers caused by unauthorised porting of mobile service numbers.

This will help prevent illegitimate access to bank accounts and other consumer service accounts—no matter which mobile carriage service provider a customer uses.

[1] ACMA *Mobile-only Australia: living without a fixed line at home*, October 2019, viewed 1 November 2019.

[2] *ACCC Submission to the Review of national arrangements for the protection and management of identity information*, November 2018, viewed 31 October 2019.

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 mobile carriage service providers.

The ACMA regulates in accordance with four principal acts—the *Radiocommunications Act 1992*, *Telecommunications (Consumer Protection and Service Standards) Act 1999, Broadcasting Services Act 1992,* and the *Telecommunications Act 1997* (the Act).

Mobile number portability

Mobile number portability is designed to promote competition by allowing customers to quickly and efficiently port between providers. In 2018–19, there were 2.55 million mobile numbers ported. Most mobile ports are completed within a few hours, and 99 per cent within two days.[3]

The rules for mobile number portability are set out in Chapter 10 of the Telecommunications Numbering Plan 2015. There are also ACMA-registered enforceable industry codes developed by Communications Alliance[4] that specify technical and operational requirements for mobile number portability, including the Mobile Number Portability Code and Telecommunications Consumer Protections Code.[5]

Under current porting requirements, the gaining mobile carriage service provider must obtain a customer's consent and authorisation prior to porting. The minimum detail required is the customer's name and address plus an account number or reference number or date of birth. For example, a port request would be accepted if a name, address and date of birth was given.

The arrangements for customer authorisation are contained in the Customer Authorisation Industry Guideline. The guideline 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.

Together, the Act, industry code and guideline provide the regulatory framework that allows telco customers to change providers without changing their mobile phone number.

[3] ACMA, *Communications report 2018–19,* 2020.

[4] Communications Alliance is the industry body for the Australian communications industry. Membership is drawn from a cross-section of the communications industry, including service providers, vendors, consultants and suppliers.

[5] The codes set out obligations for carriers and carriage service providers to obtain a customer's consent and authorisation prior to porting.

Current measures for mobile porting fraud

Mobile carriage service providers have an obligation under Part 14 of the Act to do their best to prevent their networks or facilities being used in the commission of offences against the laws of the Commonwealth, states and territories.

Communications Alliance developed an industry guidance note[6] that sets out measures for mobile carriage service providers to address the problem of mobile porting fraud.

The guidance note sits outside of the mobile portability arrangements explored above—it is an additional voluntary verification step used by industry to assist in confirming the person requesting a port is the rights-of-use holder.[7]

The government was not involved in drafting the guidance note. Compliance with an industry guidance note is not mandatory nor enforceable by the ACMA.

The guidance note identifies additional identity verification processes that gaining mobile carriage providers may complete prior to initiating a port of a customer's number.

While many Australian mobile carriage service providers have introduced stronger pre-port verification arrangements consistent with the guidance note, not all providers had committed to do so.

Those providers who have chosen to implement the guidance note voluntarily did so to assist them to reduce instances of mobile porting fraud experienced by customers.

The remaining mobile carriage service providers represent approximately three per cent of all mobile services. It is unlikely that they will adopt the guidance note measures because these providers are:

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

[6] The guidance note was made available to industry in June 2018, it is not published due to concerns about how scammers might use the information.

[7] When someone is issued a telephone number for a telecommunications service, they become a 'rights-of-use holder' for that number. This means they have a contractual relationship with a provider to use a telecommunications service or services on that number.

What is the policy problem?

Fraud

Fraud can be categorised by type or by the industry in which it occurs. The main categories of fraud in Australia include superannuation fraud, serious and organised investment fraud, mass marketed fraud, revenue and taxation fraud, financial market fraud, card fraud and identity fraud.[8]

Identity fraud is committed when a criminal uses someone else's personal information to commit a crime. 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.

The Australian Institute of Criminology estimates that one in four Australians have been a victim of identity crime at some point in their lives. Identity crime is a key enabler of serious and organised crime.[9]

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

- perpetrate frauds, including for financial gain such as removing funds from bank accounts
- establish business structures and companies to facilitate other crimes such as money laundering or importing illicit commodities
- undertake national or international travel without being identified or traced by law enforcement agencies.[10]

Responsibility for fraud is split between federal and state jurisdictions. The Australian Government is responsible for fraud against itself and its programs. Each agency is responsible for its own fraud control arrangements.[11]

The Australian Federal Police investigates most serious or complex crime against the Commonwealth, including internal and external fraud. They also conduct quality assurance reviews of agencies' fraud investigations and provide advice and assistance to entities investigating fraud. This includes recovery action under the *Proceeds of Crime Act 2002* (Cth).

State and territory governments are generally responsible for most other types of fraud. This includes responsibility for fraud against members of the public such as dating and romance scams, travel prize scams and identity theft.

[8] Australian Criminal Intelligence Commission, '*About Crime*', viewed 19 February 2020.

[9] Attorney-General's Department, '*Fraud in Australia'*, viewed 19 February 2020.

[10] Australian Criminal Intelligence Commission, '*About Crime*', viewed 19 February 2020.

[11] Attorney-General's Department, '*Government responsibility for fraud'*, viewed 19 February 2020.

Mobile porting fraud

Mobile number porting fraud occurs in the context of broader identity theft and misuse of personal information. Scammers (malicious third-party actors) gain access to personal information to exploit a necessary and legitimate telecommunications process (porting) for their own gain.

Mobile porting fraud is a crime that also acts as a gateway to broader identity and financial theft.

The government's policy objective is to prevent unauthorised ports occurring and to reduce harm to Australian consumers, as the number of potential victims of mobile porting fraud is large—anyone with a mobile phone in Australia is at risk.

Current customer authorisation processes have been inadequate in preventing mobile porting fraud. While mobile carriage service providers are not responsible for the actions of scammers, they have a role to play in prevention and reduction of harm for customers.

By improving the mobile portability regulatory framework, via enhanced pre-port verification processes, we can significantly reduce the number of Australians impacted by fraud.

Some of the impacts are captured in the four examples in this document. These draw on reports from victims of mobile porting fraud to highlight not only the financial impacts but also the psychological and emotional harms.

Example 1: I lost $6,028 when scammers stole my identity

My story*

I received an SMS informing me that my mobile number was being ported to a different network provider. As I had not authorised this, I contacted my mobile provider to find out why my number was being ported. I immediately realised what was going on and phoned my bank. While on the phone, I tried logging in to my internet banking, but to no avail. As I was talking to the bank, I started receiving emails about my personal details being changed and the PIN to the credit card being changed.

I ordered this credit card two weeks ago. It was supposed to be delivered to my address, but I have not received the card to date. I told the consultant that my credit card just got activated and that the PIN had been changed. The consultant started blocking my accounts and cards.

However, the following day when I went to the bank, they realised that the fraudster managed to lift the block and maxed out my credit card. The fraudsters have stolen my identity to create a new mobile account at the different network provider, hacked my internet banking account, and stolen funds.

**The example above is based on one or more real scam reports received by the Australian Competition and Consumer Commission.*

How mobile porting fraud occurs

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 capable of receiving personal information, such as unique verification codes.

Scammers commit identity theft or use a person's online information to fraudulently appear to be the rights-of-use holder in order to complete a customer authorisation. They then request a port to a new mobile carriage service provider—allowing them to gain control of the mobile service number.

The process is fraudulent because the scammer is not the rights-of-use holder and has impersonated the legitimate customer to gain access to a benefit—the mobile service number (and associated sensitive information accessed via the mobile phone).

The legitimate customer—the rights-of-use holder—may not receive any notification of the port occurring so may not be aware that this fraudulent activity has happened until their mobile phone loses coverage and they contact their provider.

When the ported mobile service activates, the scammer will receive all the legitimate customer's SMS messages and calls. The scammer can then use the mobile phone number to access bank accounts and other applications containing sensitive information that use two-factor identification methods[12]. For example, using maliciously obtained personal information to target bank account/s, and using the confirmation code sent to the mobile number to transfer funds from the account/s.

If a customer has been the victim of mobile porting fraud, they need to take steps to regain their number (reverse the port) and establish their identity with their mobile carriage service provider. They will also need to recover financial losses (if possible) with their financial institution—and deal with other issues arising from the identity theft.

Mobile porting fraud victims often need to use support services like IDCARE for advice on re-establishing their identity with government services or financial institutions. This may require presenting in person with photo-identification to multiple government services or banks, which is a time-consuming process.

Who is affected by mobile porting fraud?

Mobile porting fraud can happen to anyone with a mobile service number. At June 2019, there were 35.82 million[13] mobile services in operation—each a potential target for scammers. While vulnerable members of society are often the target of scammers, anyone can be affected by mobile porting fraud.

Businesses impacted by fraud can suffer significant losses due to the costly impact of disruption to essential mobile services and potential business assets lost through fraud. Customers are losing trust in Australian telecommunications providers to protect

[12] 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). The use of mobile phones for two-factor authentication means scammers can use the ported number to access bank accounts, social media, online businesses, government services such as myGov and any other account which uses the phone as a secondary security check.

[13] ACMA, *Communications report 2018–19*, 2020.

them from mobile porting fraud and are frustrated that they have no means to protect themselves.

Customers 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.[14]

Example 2: Fraudsters strike quickly with mobile porting fraud

One Tuesday night around 7 pm, Debbie* received a text from BlueTel telling her that her mobile number had been ported across to a different carrier. The message urged Debbie to call BlueTel if she didn't request for her number to be ported out. But it was already too late. Her mobile phone service had already stopped.

Not long after this, Debbie received notifications from her bank app confirming transactions she didn't make, including withdrawals of cash and online purchases.

Debbie is a small business owner with several business bank accounts used for clients and staff. She had to freeze all of them, as well as her own personal bank accounts to prevent further theft. This meant she was unable to pay her staff.

She spent all Tuesday night trying to stem the damage done to her business and get her mobile number back, which had already been moved across to BlackTel.

The next morning, she went into the BlueTel store and was told it would take four days to get her number back. She was told a woman had stolen her identity, but BlackTel staff could not tell her any other details.

Debbie said, 'It's been a nightmare for me, my staff and my business. BlueTel blames BlackTel. My bank blames BlueTel. And BlackTel blames BlueTel. It's been a massive inconvenience and no one else should have to go through this'.

**Example is based on one or more reports of mobile porting fraud. Names of individuals and companies have been changed.*

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

Why is government action needed?

ACMA consumer research confirms scams over telecommunications networks are a significant problem, and telco customers expect more to be done by government.[15] Australians lose more than half a billion dollars a year to scams and that number is increasing.[16]

Combating telecommunications scams is a government priority. The Minister signed off on the ACMA's Combating Scams Action Plan in November 2019. The Australian Government wants all mobile service providers to implement stronger pre-port identify checks, to minimise instances of fraudulent mobile number porting and reduce associated financial loss and hardship to customers.

Government action is needed now to coordinate and enforce community-wide customer protection measures. Without this action, all Australian mobile users are at increasing risk of mobile porting fraud.[17]

Market action

Australia's communications landscape continues to undergo exponential change. In the past decade developments in digital products and services have reshaped business models, global markets, consumer experience and expectations.

With technology rapidly evolving, the use of multi-factor authentication for accounts has become more prevalent. There is increasing interest in stealing phone numbers because banks often send two-step verification codes over SMS.

In addition to rising financial losses from scams, a 2016 report from the Attorney-General's department estimated identity crime cost Australians $2.2 billion per year.[18] The implications of fraudulent number porting for mobile customers can be very serious and include but are not limited to financial loss, negative credit ratings, psychological harm and emotional stress. Once a customer has had their identity stolen, it can be very difficult and time-consuming to reverse the effects.

The telecommunications industry initially categorised mobile porting fraud as a financial services industry issue for relying on mobile phones for two-factor authentication. However, major services such as social media, email providers and government agencies now use mobile phones for password resets and multi-factor identification purposes.

All three carriers and most major resellers representing approximately 97 per cent service coverage or over 34 million mobile services[19] have (or have committed to

[15] ACMA, *Unsolicited calls in Australia: Consumer experience*, 2018, viewed 17 December 2019.

[16] The ACCC reports losses to scams will exceed $532 million by the end of 2019. Scamwatch, 'Record losses expected as scammers target Australians', 2019, viewed 17 December 2019.

[17] ACCC, Consultation submission 2020.

[18] Attorney-General's Department, *Identity crime and misuse in Australia* 2016.

[19] 35.82 million mobile services in operation as of June 2019 as reported in ACMA *Communications report 2018–19*, 2020.

implementing) verification measures to address unauthorised ports in-line with the industry guideline.

However, not all mobile carriage service providers have acted to adopt processes to confirm that the person initiating the port holds the rights of use to that number. And that gap in protections creates an opportunity for scammers, which has consequences for all customers.

More can be done to address the problem of mobile porting fraud—but government action will provide the strongest incentive to achieve the best outcome for the Australian community.

What policy options have been considered?

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

1. Status quo

The government maintains the status quo by not introducing any new form of regulation—existing legislation and regulations (including the Numbering Plan, Mobile Number Portability Code, and Customer Authorisation guidelines) remain.

Communications Alliance encourages mobile service providers to act in accordance with the industry guidance note, with members deciding whether to comply. Those who use pre-port verification processes apply them in addition to existing laws and regulations to help them to prevent instances of mobile porting fraud.

The guidance note addresses mobile porting fraud by adding an additional verification step prior to a gaining mobile carriage service provider accepting a port. The verification step involves, for example, the use of multi-factor identification (for example, use of an SMS code) to check the identity of a person requesting a port. This assists mobile carriage service providers to ensure the rights-of-use holder has requested the port.

The ACMA has no compliance or enforcement powers in relation to the guidance note.

2. Education campaign

The government does not introduce any new form of regulation but conducts a targeted public education campaign that provides clear and accessible information about mobile porting fraud. The existing legislation and regulations (including the Numbering Plan, Mobile Number Portability Code, and Customer Authorisation guidelines) remain.

The campaign is run by the ACMA in accordance with usual practice. This involves:

- information on the ACMA website
- a short, engaging video providing customers with relevant information in an accessible format, with a production budget of $10,000 to $15,000
- targeted ads on Facebook to reach consumers (an image, post content and link back to the ACMA website)
- use of LinkedIn to reach mobile carriage service providers
- use of direct email lists and line area industry contacts
- a budget of $5,000 to $10,000 to boost impressions of the social media content.

Campaign activities are also undertaken in collaboration with other government agencies, consumer advocacy groups and mobile carriage service providers. These include using websites and social media channels, issuing emails/letters/bulletins, and stakeholder and community forums. Information is provided to culturally and linguistically diverse communities and vulnerable customers.

Engagement activities inform mobile customers about the risks of mobile porting fraud and the use of additional verification measures—without providing scammers with too much information about how to circumnavigate the verification process.

The campaign advises customers how to improve their mobile phone security and what to do if they become a victim of mobile porting fraud and empowers them to make informed choices about providers through general consumer awareness tools and templates. However, some members of the community may still not receive nor understand the campaign information.

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

The industry guidance note remains in accordance with the status quo; however, education campaign activities incentivise voluntary compliance. More mobile carriage service providers view voluntary additional protections as part of their duty to do their best to prevent their networks or facilities being used in commission of criminal activity.

The ACMA has no compliance or enforcement powers in relation to the guidance note.

3. Industry standard (s125AA Telecommunications Act)

The government introduces new regulation in the form of an industry standard that requires gaining mobile carriage service providers to implement additional identity verification before they port a mobile service number.

The ACMA *may* determine an industry standard under Part 6 of the Act in limited circumstances. This includes where it has requested an industry body 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). An industry code is drafted by a representative industry body and registered by the ACMA.

The ACMA *must* determine an industry standard if directed by the Minister in accordance with section 125AA of the Act.

An industry standard applies to participants in a particular section of the telecommunications industry; and deals with one or more matters relating to the telecommunications activities of those participants.

Compliance with an industry standard is mandatory.

An industry standard is an enforceable legislative instrument with enforcement options under the Act including formal warnings and civil penalties of up to $250,000.

The industry standard option sets out pre-port identity verification processes for gaining providers to use prior to accepting the port of a number. It is new regulation and is additional to the identity verification requirements in the mobile number portability regulatory framework, including the Numbering Plan, Mobile Number Portability Code, and Customer Authorisation guidelines.

The standard draws on identity verification processes already voluntarily adopted by some of the industry. These processes are practicable, robust, technically feasible and do not impose undue financial and administrative costs. The verification methods are

used to match the identity of the person requesting a port with the rights-of-use holder of the mobile number to be ported.

These identity verification methods include:

- use of biometric data
- multi-factor authentication
- use of documents (for limited circumstances).

The industry standard requires mobile carriage service providers to publish customer information on their website.

This option allows for mandatory, enforceable provisions that will provide community-wide protection against mobile porting fraud.

What is the likely net benefit of each option?

1. Status quo

Benefits

Mobile carriage service providers without resources to implement pre-port verification measures may benefit from choosing not to implement any additional verification methods as set out in the voluntary industry guidance note.

In addition, these same businesses are likely to gain a benefit from the purchase of their post- or pre-paid services by scammers who can continue to port a number to a new provider without additional security. This benefit is likely to be limited to the initial cost of purchase—as scammers retain the service only long enough to complete identity theft, for example, the initial purchase of a $10 pre-paid SIM.

Costs

Reported incidents

Mobile porting fraud is both under-reported and inconsistently reported. Fraud victims may report to none, one or all of the government or consumer agencies that take reports—such as the ACMA, Australian Competition and Consumer Commission (ACCC), Telecommunications Industry Ombudsman (TIO), IDCARE and the Australian Cyber Security Centre.

Between July 2017 and September 2018, mobile carriers Optus, Telstra and Vodafone reported 2,585 mobile porting fraud complaints to the ACMA—approximately 2,068 complaints annually.

During 2017–18, IDCARE's[20] community crisis support services responded to 1,056 engagements involving the unauthorised porting of a mobile phone service.[21] It is unclear how many of these engagements are captured in the complaint numbers reported to the ACMA or if all losses have been accounted for.

For consistency, the figures reported directly to the ACMA by mobile carriage service providers will be used to assess the impact of mobile porting fraud. Due to the inconsistent reporting patterns, it is likely our estimate will not capture the full scope of the problem.

Financial losses

Mobile carriage service providers do not have information on financial losses attributed to mobile porting fraud; however, IDCARE suggest that one in three victims of mobile porting fraud experienced financial loss, with an average loss of $11,368.[22]

This represents an estimated financial loss of $7,848,749.33 in the 2017–18 financial year.[23]

---

[20] IDCARE is Australia and New Zealand's national identity and cyber support service—formed to address a critical support gap for individuals confronting identity and cyber security concerns.

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

[22] ibid.

[23] Figure based on 2,068 fraud complaints / 3 * $11,368 = $7.8m.

If the status quo is maintained, it can be anticipated that the levels of financial losses attributed to mobile porting fraud will continue to increase as scammers become more efficient at targeting customers. There is also the cumulative impact from ongoing identity theft as scammers use the ported number to gain further personal information for later use.

Assuming customers quickly notify their financial institution, the financial cost of fraud may be borne by those institutions—with customers recovering money lost through fraud protection policies.[24]

While it is difficult to predict the losses in 2020, data from ACCC's Scamwatch gathered between 1 Jan and 15 Dec 2019 demonstrated a 508 per cent increase in financial losses due to mobile porting fraud. Over that same period, the number of cases reported to the ACCC rose by almost 30 per cent. [25]

During the same period, financial losses (from reports to Scamwatch about 'attempts to gain your personal information') rose by nearly 70 per cent—indicating the trend in financial losses associated with identity theft is increasing.[26]

While an increase in financial losses in 2020 is anticipated, the figures provided are conservative (estimating a 20 per cent increase in losses per victim)— compared to the ACCC data that suggests a potential 508 per cent increase in financial losses from mobile porting fraud (rising from $134,666 in 2018 to $1,058,061 in 2019).[27]

Based on these figures, an estimate for mobile porting fraud cases in 2020 is 2,688.[28]

Assuming one in three victims suffer financial losses (IDCARE), and the losses start at $11,368 per person (IDCARE), a 20 per cent increase would put losses per victim at $13,642—and total losses just under $12.2 million.[29]

Costs to mobile carriage service providers

Mobile carriage service providers spend time and resources responding to instances of mobile porting fraud and assisting their customers to manage the impact and recover their services.

Time is spent on training frontline staff on how to identify potential fraud cases (for example, mobile porting fraud is often identified because a customer says they are not getting service) and resourcing specialist fraud teams to address the fraud when it occurs.

Costs to businesses

The impact on businesses from mobile porting fraud is often higher than that experienced by individual customers.

As reported by the Australian Institute of Criminology, a criminal syndicate targeted retail businesses by fraudulently porting the phone of the business owner or manager. With access to the number, they contacted staff to prepare stock for collection by a courier who would quickly collect the goods before staff realised the request had not

[24] ANZ policy https://www.anz.com.au/security/account-protection/fraud-money-back-guarantee/

[25] ACCC Consultation submission 2020.

[26] ibid.

[27] ibid.

[28] Figure based on a 30 per cent increase on annual cases reported to ACMA (2068 cases).

[29] Figure based on 2,688 fraud complaints /3 * $11,368 *1.2 = $12.2m.

come from the owner. The scam was successful on 25 occasions before members of the syndicate were arrested and charged. The value of this fraud was over $1 million[30]—it is unknown how many other similar instances there might be.

The ACMA is also aware of instances of mobile porting fraud designed to interrupt business activity, for example, by depriving key staff of their ability to communicate or disrupting time-sensitive transactions.

Costs of identity theft

While 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.

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

In figures for 2017–18, IDCARE estimated that an average of 32 hours is spent by customers to address identity theft.[31] These figures do not include lost productivity where a customer has taken time off work to address identity theft.

Calculated at the OBPR leisure labour rate of $32 per hour for private citizens (and based on an estimate of 2,688 complaints in 2020), this represents a minimum cost of $1,024 per victim—or total losses of $2,752,512 per year.

Victims of identity theft can also experience multiple instances of fraud over months or years.[32] Support service IDCARE recommends victims set up yearly reporting to allow for continual monitoring. Identity theft has long-term, unquantifiable repercussions for victims.

But the impact of mobile porting fraud on customers whose identity is stolen goes beyond economic losses suffered.[33] Identity theft affects more than just any single individual. The fraud can impact those close to victims, with financial and psychological stress involved. In some extreme cases, victims have difficulties in finding employment, are refused services or are refused credit due to the fraud.[34]

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

---

[30] Australian Institute of Criminology, *Identity crime and misuse in Australia 2017.*

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

[31] Australian Institute of Criminology, '*Identity crime and misuse in Australia'*, 2017, viewed 9 January 2020, page xi.

[32] ibid.

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

[34] Australian Institute of Criminology, '*Identity crime and misuse in Australia'*, 2017, viewed 9 January 2020, page xiv.

Example 3: Identity theft takes an emotional toll

Cate* had her number ported from BlueTel to WhiteTel without authorisation after her driver's licence was compromised.

Within 10 minutes of receiving a text notifying her that her number was to be ported, her phone had stopped sending or receiving text messages and phone calls. By the time she was able to check her accounts, the scammers had accessed her email, bank account, Facebook and committed fraud—transferring nearly $10,000 out of her account.

For weeks afterwards, she could not sleep properly, and was constantly checking her phone, emails and social media accounts for more attempts to take control. While the financial loss has been significant, Cate said the ongoing feeling of persecution and not being able to trust anyone has been the worst aspect of the fraud.

'The emotional stress from being borderline paranoid when anyone asks for any personal information for any reason is overwhelming at times. Feeling exposed and unsafe doesn't just go away.'

**The example above is based on one or more real mobile porting fraud reports. The identities of victims and some details have been changed.*

Gateway to further fraud

There are a range of organisations that actively use codes or confirmation links sent to mobile numbers:

- banks and financial institutions
- superannuation funds
- technology companies
- health booking services
- social media
- airlines and transport companies
- online retailers
- delivery services
- email providers
- energy and utility companies.

Organisations that use mobile phones for their own multi-factor authentication checks face a secondary cost where mobile porting fraud occurs. They are disadvantaged by needing to mitigate the effects of mobile porting fraud on their customers and expending the resources required to do this.

Mobile porting fraud is a security risk to the services they offer. In some cases, mobile porting fraud of one customer also impacts another customer using that service; for example, access to one social media account may provide a gateway to identity theft of other customers using that service.

This represents both a security and reputational risk for the telecommunications industry and for all organisations that rely on mobile phones for multi-factor authentication.

Example 4: The social network

Andrew* recently had his phone ported without his knowledge or consent. The scammer used the mobile number to access Andrew's Facebook page and impersonated Andrew to contact his friends.

The scammer asked five of Andrew's friends to be a referee for a bank loan. Andrew's friend Beth offered to help. After giving information to the scammer, Beth's phone was also fraudulently ported. The scammer accessed Beth's bank accounts, made a new account to transfer funds into, opened a currency card to spend worldwide and increased Beth's credit limit. The scammers ended up with over $12,000 of Beth's money.

Beth got most of the money back after contacting the banks and cancelling online purchases. As a result of the fraud, she felt violated.

**The example above is based on an instance of mobile porting fraud reported in the media. The identities of victims and some details have been changed.*

2. Education campaign

Benefits

An education campaign will support customers to be aware of mobile porting fraud, enhance their knowledge of their rights and responsibilities and assist them to avoid poor choices.

Informed customers are more likely to better protect their personal information, which will help prevent identity theft—the key factor needed to complete a fraudulent port—and reduce the significant distress, trauma and suffering that occurs due to mobile porting fraud and the accompanying identity theft.

Customers will be empowered to protect themselves from mobile porting fraud and know how to respond in the event of an authorised port—for example, by taking control of how they share their personal information in public and quickly contacting their financial institution and mobile carriage service provider if they experience an unauthorised port.

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 mobile carriage service providers what they are doing to prevent mobile porting fraud before choosing their provider.

This may incentivise mobile carriage service providers to voluntarily increase protections, which may also reduce instances of mobile porting fraud. For example, a provider who voluntarily implements multi-factor identification will make it harder for a scammer to successfully impersonate a rights-of-use holder.

Education campaign activities will enhance mobile carriage service providers' (particularly smaller providers) understanding of their regulatory responsibilities to both customer and the regulator. Stronger application of existing authorisation guidelines may prevent some instances of fraud where a scammer has incomplete information to complete a port (for example, name and address but not date of birth).

For this assessment, it is anticipated that coverage of pre-port verification measures will rise to voluntarily cover 97 to 98 per cent of mobile carriage services, in line with commitments provided by the telecommunications industry.

The practical impact of an education campaign could result in an estimated 20–30 per cent reduction in mobile porting fraud cases compared to the status quo. This reduction is due to the increase in voluntary protections and the impact of informed customers.

In 2020, the benefits of this reduction represent:

- a decrease in mobile porting fraud cases from 2,688 to between 1,882 and 2,150
- a decrease of 20–30 per cent in instances of psychological harm caused by porting fraud, and the need for customers to seek support services
- savings of financial losses to mobile porting fraud of between $2.4m[35] to $3.7m[36]
- savings in time spent by customers responding to identity theft of between $550,000[37] to $825,000[38]
- freeing up of telecommunication fraud team resources to assist customers on other matters (currently equivalent to 20–30 per cent of their time)
- a reduction in the resources required by community organisations (such as IDCARE) assisting customers who have experienced identity theft relating to mobile porting fraud (equivalent savings of 20–30 per cent).

Benefits would also be experienced by businesses and organisations that rely on use of a mobile phone for multi-factor authentication as a security factor for their services.

An educational campaign would have reputational benefits for the mobile telecommunications sector—particularly for mobile carriage service providers that can demonstrate their commitment to protections for their customers.

Costs

Costs to customers

There are no direct costs to customers from an education campaign; however, the costs to customers come from remaining instances of mobile porting fraud. The following costs remain for the estimated 1,882 to 2,150 cases of mobile porting fraud in 2020:

- psychological harm and distress for each instance of mobile porting fraud and ongoing repercussions of identity theft
- financial losses of approximately $8.6m[39] to $9.8m[40]
- cost of time spent by customers responding to mobile porting fraud of $1.9m[41] to $2.2m[42]
- expenditure of the remaining 70–80 per cent of resources for community organisations (such as IDCARE) in assisting customers who have experienced identity theft relating to mobile porting fraud.

[35] Figure based on 538 fraud complaints /3 * $11,368 *
1.2 = ~$2.5m.

[36] Figure based on 806 fraud complaints /3 * $11,368 *1.2 = ~$3.7m.

[37] Figure based on 538 fraud complaints * 32 hours * $32 = ~$0.55m.

[38] Figure based on 806 fraud complaints * 32 hours * $32 = $0.825m.

[39] Figure based on 1882 fraud complaints /3 * $11,368 *1.2 = ~$8.6m.

[40] Figure based on 2150 fraud complaints /3 * $11,368 *1.2 = ~$9.8m.

[41] Figure based on 1882 fraud complaints * 32 hours * $32 = ~$1.9m.

[42] Figure based on 2150 fraud complaints * 32 hours * $32 = ~$2.2m.

Costs to industry
Mobile carriage service providers may need to direct resources towards implementing additional stakeholder engagement activities and updating existing information to align with educational activities.

All mobile carriage service providers remain susceptible to the impacts of mobile porting fraud. The process of mobile porting involves moving away from an existing provider, so if provider A and B have additional protections but provider C does not, customers with both A and B can continue to be fraudulently ported to C. Therefore, the gap in providing community-wide protections remains.

Better informed customers may also increase workloads for fraud teams—as customers will be more responsive to the signs of fraudulent porting. Mobile carriage service providers will continue to need to spend time and resources responding to mobile porting fraud as well as assisting their customers to manage the impact and recover their services.

Time is also spent on training frontline staff or resourcing specialist fraud teams on how to identify and address potential fraud cases. For example, mobile porting fraud is often identified because a customer says they are not getting service, which is most often because their number has been ported.

Reputational costs are less than the status quo but still impact the perception of mobile carriage service providers by their customers and other businesses relying on mobile phones for multi-factor authentication.

3. Industry standard

Benefits

For this assessment, it is anticipated that coverage of pre-port verification measures will rise from mobile carriage service providers covering 97 per cent of mobile services to 100 per cent of mobile services when the standard commences.

An industry standard provides a consistent, community-wide approach by establishing processes and protections that allow for certainty for both mobile carriage service providers and their customers. With all mobile carriage service providers treated the same, there is a competition benefit.

An industry standard can address the regulatory gap by imposing an enforceable obligation on a gaining mobile carriage service provider to verify the identity of the customer seeking to port their number. A losing mobile carriage service provider may have additional protections, but this will not protect customers who are porting to a gaining provider that does not. If mobile carriage service providers remain who do not have protections, scammers are incentivised to port to those providers, even if a majority of providers *do* have protections.

The additional protections offered by mobile carriage service providers become more effective as scammers lose the incentive to target providers without protections. If all providers have protection, no customer can be ported away without a process of additional identity protection.

Mobile carriage service providers that have already implemented the measures set out in the industry guideline have found them to be practicable, robust and technically feasible. This experience has directly informed mandated obligations in the standard. Data suggests these measures reduce mobile porting fraud by up to 96 per cent for

individual providers.[43] With coverage across all mobile carriage service providers, this figure is likely to increase.

Customers can expect to benefit from an industry standard that mandates additional security measures. While no anti-fraud measure can be assumed to be completely effective, a conservative 90 per cent drop in porting fraud cases has been estimated to test the benefit of industry-wide coverage.

The most significant benefit of an industry standard would be a reduction of mobile porting fraud cases in 2020 and beyond. It is estimated these would be reduced from 2,688 (if the status quo is maintained) to 267 cases per annum.

This represents roughly 2,419 customers who would not face the distress, trauma and suffering that occurs due to mobile porting fraud and the accompanying identity theft. This benefit is difficult to articulate given the potential breadth and scope of harm, and the ongoing impacts of identity theft often being felt for years after the initial event.

Overall, a 90 per cent reduction in mobile porting fraud cases compared with the status quo in 2020 represents:

- a 90 per cent decrease in instances of psychological harm and the need for a customer to seek support services
- savings of $11m[44] in losses to mobile porting fraud
- savings of $2.5m[45] in time spent by customers responding to identity theft
- an equivalent of 90 per cent of telecommunications fraud team resources used in responding to mobile porting fraud issues being freed up to assist customers on other matters
- a saving equivalent of 90 per cent of the resources expended by community organisations (such as IDCARE) in assisting customers who have experienced identity theft relating to mobile porting fraud.

An industry standard provides both customers and industry with certainty in the approach to mobile porting fraud. It addresses an information asymmetry, where providers know which provider has additional protections, but customers do not have this information unless they request it.

The industry standard has broader benefits for organisations that use mobile phones for their own multi-factor authentication checks. The reduction of mobile porting fraud by 90 per cent makes the mobile number a more reliable method of authentication and would similarly reduce the instances of secondary fraud experienced on their platforms. It would also reduce the resources needed to rectify accounts and assist customers.

Finally, there is a reputational benefit for mobile carriage service providers when their services are viewed as more safe and secure. This will come both from customers who are satisfied with extra protections and businesses who appreciate the secondary protections afforded to their customers through the standard.

[43] Figure reported to ACMA by one mobile carriage service provider that has an established pre-port verification solution.

[44] 2,419 fraud complaints /3 * $11,368 *1.2 = $11m.

[45] 2,419 fraud complaints * 32 hours * $32 = $2.5m.

Costs

Costs for customers

Customers may face a time burden that did not previously exist when they port their number. This could dissuade them from requesting a port. For example, responding to an SMS takes approximately 30 to 60 seconds. This cost is not substantive unless a customer does not know action is required and fails to take any action, delaying the port for longer.

Feedback during and prior to consultation suggested this time burden can be exacerbated if mobile carriage service providers do not communicate that the customer must complete the verification to proceed with their port.

Costs for industry

For mobile carriage service providers, the main cost associated with an industry standard is likely the implementation of potential new IT systems or procedures, and training staff in those systems. Although most mobile carriage service providers have completed implementation (or are in the process of voluntarily doing so), there are still providers—covering approximately three per cent of mobile services—who will need to meet this initial cost.

Consultation did not provide significant insight into potential implementation costs. One major mobile carriage service provider advised the cost of compliance with the industry guidance note was approximately $1 million.[46]

Using the OBPR labour rate of $73.05 per hour, estimated costings for a manual SMS or phone call verification process to be completed is between $82,912 and $465,694 per annum. This represents the time spent by a staff member (one to five minutes) to complete verification for those services (three per cent of ports per annum), which would now be covered by an industry standard.

However, by providing a degree of flexibility in the verification measures for a pre-port process in the standard, (such as allowing mobile carriage service providers to align it with their existing systems), the cost of change is mitigated.

It is likely that any regulatory cost burden will be greater on smaller mobile carriage service providers that are less likely to be able to absorb the initial outlay. Yet these are the providers that most need to implement the changes to close incentives for scammers to port into providers without additional protections.

Some mobile carriage service providers that haven't had additional protections will lose the insignificant benefit of being the scammers' gaining provider of choice, and the business income this generates. It is expected that smaller providers (or those that haven't voluntarily implemented protections) will be disproportionately affected.

If customers are not charged for verification SMS responses, industry will need to bear this cost (cost of SMS will be less than the retail price, but the exact cost for industry is unclear). The management and implementation of a system to achieve this (such as a process to record the agreed free-rated numbers) will be left for industry to determine based on their systems and existing relationships.

[46] Figure based on one submission and may not be indicative of all mobile carriage service providers given some may have already implemented systems and processes, and each vary in size of operation.

Finally, a potential cost of closing incentives for scammers to exploit mobile porting is the risk of them moving to similar, but less protected, processes.

Regulatory burden measurement table

Option	Regulatory cost
Status quo	n/a
Education campaign	n/a
Industry standard	$465,694*

The industry standard is expected to cover the three per cent of annual ports that are not already covered by mobile carriage service providers that have implemented (or who have committed to implement) the measures set out in the industry guidance note. There is no new regulatory burden on mobile carriage service providers that have already implemented (or who have committed to implement) the measures in the industry guidance note.

In the absence of specific data on implementation costs, we anticipate that the regulatory burden for mobile carriage service providers that have not yet implemented (or committed to implementing) additional identity verification measures to comply with the industry standard is around $465,000*. This assumes compliance is achieved by manually notifying customers via SMS when a porting request is made, and that verification of each port request would take five minutes on average.

The calculation* is derived below:

76,500 ports per year (three per cent of 2.55m annual ports not covered by the guidelines) * five minutes / port @ $73.05 / hour.

Who was consulted and what did they say?

Consultation

The ACMA has been kept informed by Communications Alliance on industry measures to address mobile porting fraud over time, including exploration of the Jersey solution[47] and development of the industry guidance note. The ACMA has regularly sought data on complaint numbers to understand the magnitude of the issue and information about any actions taken by carriers to address mobile porting fraud.

When industry began implementing the voluntary guidance note, the ACMA tracked progress of implementation and the rate of industry coverage of voluntary measures.

The ACMA has similarly engaged with IDCARE and the Australian Communications Consumer Action Network (ACCAN) on their complaints data to understand their view of the problem. The TIO and the Australian Criminal Intelligence Commission have both provided data to inform the ACMA's consideration of the problem.

Post-October 2019

The ACMA met with mobile carriers to better understand existing industry practices and how they could be reflected in an industry standard. We referred to the industry guidance note prepared by Communications Alliance and the outcomes of the consultation that had occurred prior to a Ministerial direction.

Full public consultation on a draft industry standard was conducted from 6 December 2019 to 19 January 2020.

This included targeted consultation with key members of industry, government and consumer groups to give wide opportunity for affected stakeholders to give input. We informed key stakeholders of the publication of the documents and invited comment on the draft of the industry standard and on the issues set out in the consultation paper. Social networking sites were used to raise public awareness of the consultation and complemented online consultation.

The ACMA must comply with statutory consultation obligations prior to making an industry standard. Statutory consultation provisions in subsection 125AA(3) and sections 132, 133, 134, and 135 of the Act have been met through:

- a public notice published in *The Weekend Australian* on 7 December 2019—a newspaper that circulates in each state and territory
- public consultation for a period of 45 days including the Christmas and New Year holidays[48]
- consultation with the ACCC, the TIO, the Office of the Australian Information Commissioner (OAIC), telecommunications industry bodies, Communications Alliance and the Australian Mobile Telecommunications Association, and two consumer bodies—ACCAN and IDCARE.

[47] The Jersey solution refers to an intermediary service that would give real-time mobile number transfer and porting information to banks. The bank could use the data to help detect and mitigate subsequent fraudulent activity, but it has no impact on the porting process.

[48] Legislative requirement for minimum of 30 days.

Summary of stakeholder feedback

The consultation sought comment on several key requirements that the ACMA was considering including in the industry standard as well as inviting general comments.

The ACMA received 14 submissions from a range of stakeholders:

- two victims of mobile porting fraud
- three mobile carriers—Optus, Telstra and Vodafone
- mobile resellers Woolworths and iiNet/TPG
- industry body Communications Alliance
- peak communications consumer organisation ACCAN
- government agencies—the ACCC, the Digital Transformation Agency (DTA), the Department of Home Affairs, OAIC and the TIO.

All submissions supported an industry standard being made to address mobile porting fraud.

Consultation submissions focused on the proposed requirements:

- flexibility of pre-port verification measures
- application of pre-port processes to customer types
- balance between security and accessibility of pre-port verification process
- cost of verification options for customers
- inclusion of customer awareness and safeguard information.

These issues and editorial feedback provided in all submissions has been considered.

What is the best option from those considered?

An industry standard determined under section 125AA of the Act is the best option and has the highest net benefit of options considered. Consultation feedback suggests an industry standard is supported by mobile carriage service providers, individuals, government and community organisations.

The industry standard is enforceable and enables the ACMA to monitor and enforce compliance. This removes incentives for scammers to target providers without additional protections and provides certainty to customers that they are protected from mobile porting fraud.

An industry standard also provides more robust protections for customers through consideration of practicable, robust, technically feasible verification measures. These protections do not impose undue financial and administrative burdens on mobile carriage service providers but improve protections.

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

The education campaign option has some benefits to customers and mobile carriage service providers; however, it does not match the benefits of an industry standard.

How will you implement and evaluate your chosen option?

Implementation

Most mobile carriage service providers have already implemented (or are committed to implementing) additional identity verification processes. Learnings from this have been incorporated into the drafting of the industry standard through both formal and informal consultation.

Option 3—an industry standard—will be implemented by the ACMA in accordance with a Ministerial direction that the standard must be determined by 28 February 2020 and commence by 30 April 2020. This provides time for remaining mobile carriage service providers to put systems in place to achieve compliance with the standard.

Engagement with stakeholders

The ACMA will lead government engagement with key stakeholders to ensure they are aware of their new regulatory obligations.

Mobile carriage service providers must implement pre-port identity verification processes, but the standard is drafted with in-built flexibility to allow choice in methods used to comply. This will minimise the costs of upgrading systems and support entities that have already implemented solutions from the guidance note to continue implementation or use of their chosen method.

The ACMA will work with mobile carriage service providers where implementation issues are identified. For example, the consultation highlighted that providers using an SMS verification method found customers were unable to complete verification if they had no pre-paid credit. The standard will be drafted to avoid this implementation issue by mandating that customers do not pay for a verification SMS response. This prompts industry to determine its own cooperative arrangements to zero-rate SMS (that is, sending the SMS without cost). The industry has until the commencement of the standard to determine the most effective way to do this.

The consultation did not indicate any particular issues with implementation of staff training to process pre-port verifications and it is expected that each mobile carriage service provider will take the necessary steps to ensure staff are ready to complete the new processes at the commencement of the industry standard.

Customer awareness and safeguard information is expected to be straightforward to implement, with mobile carriage service providers stating they already cover much of the information on their websites and would make updates to meet the requirements of the standard.

Education campaign

The ACMA has a range of regulatory tools to encourage compliance, such as education of industry and customers. While an education campaign did not have the greatest net benefit as a standalone option to address mobile porting fraud, a modest 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 pre-port verification processes.

Evaluation

Through compliance activities, the ACMA will monitor and evaluate the success of the industry standard and can vary it should the measures prove ineffective.

The ACMA will have an active compliance work program for the industry standard. This will include monitoring of complaints about mobile porting fraud received by the TIO and escalation processes where appropriate, including potential investigations and enforcement activities.

Additionally, the newly formed Scam Telecommunications Action Taskforce (STAT) will monitor the impact of the standard. The STAT is responsible for actions on telecommunications scams following the release of the *Combating Scams* action plan[49] and will be well placed to evaluate the success of the measures in the standard.

The STAT is chaired by the ACMA and includes members from government (the ACCC; the Department of Infrastructure, Transport, Regional Development and Communications; and, the Australian Cyber Security Centre) as well as Communications Alliance (and its members). Other relevant parties such as law enforcement, government agencies and financial institutions with observer status also participate where issues are relevant to them.

[49] ACMA, *Combating Scams* action plan, November 2019.