New rules to prevent fraud from unauthorised customer interactions
with telecommunications providers

Proposal to make the Telecommunications Service Provider (Customer Identity Verification) Determination 2021

NOVEMBER 2021

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

Copyright notice



<https://creativecommons.org/licenses/by/4.0/>

With the exception of coats of arms, logos, emblems, images, other third-party material or devices protected by a trademark, this content is made available under the terms of the Creative Commons Attribution 4.0 International (CC BY 4.0) licence.

We request attribution as © Commonwealth of Australia (Australian Communications and Media Authority) 2021.

All other rights are reserved.

The Australian Communications and Media Authority has undertaken reasonable enquiries to identify material owned by third parties and secure permission for its reproduction. Permission may need to be obtained from third parties to re-use their material.

Written enquiries may be sent to:

Manager, Editorial Services
PO Box 13112
Law Courts
Melbourne VIC 8010
Email: info@acma.gov.au

Executive summary 1

Matters for comment 2

The draft determination 3

Preventing fraud from high-risk customer interactions 3

Key matters for consideration 4

Invitation to comment 9

Making a submission 9

Executive summary

The Australian Communications and Media Authority (the ACMA) is consulting on proposed new rules to prevent unauthorised customer interactions involving telecommunications services and accounts. This will help reduce the harms to consumers from fraud.

Scams over telecommunications networks are a significant problem, causing financial and emotional harm to victims and undermining confidence in networks. Scams are predominantly being perpetrated by malicious third-party actors based offshore.

Scammers are also increasingly finding ways to target weaknesses in existing customer identity verification processes. They are technologically adept, increasingly sophisticated and show no signs of stopping.

In February 2020, we made the the [Telecommunications (Mobile Pre-Porting Additional Identity Verification) Industry Standard 2020](https://www.legislation.gov.au/Details/F2020L00179) (the PPV Standard). It addresses the harms caused by mobile porting fraud by requiring mobile providers to use additional identity verification methods before a mobile number is ported from one provider to another.

There is strong evidence that the implementation of the PPV Standard has led to a significant drop in fraudulent number ports. Most stakeholders in government, the telecommunications industry and financial services sector have reported significant drops in reported fraud cases since its introduction.

Unfortunately, reports from all stakeholders indicate that there are significant ongoing harms from scammers targeting SIM swap[[1]](#footnote-2) processes. ACMA analysis indicates that more than 80% of mobile number fraud between January and May 2021 resulted from SIM swaps.

We are also aware of emerging harms as scammers target other customer interactions with telecommunications providers to facilitate identity and financial theft. Other points of vulnerable customer interactions include billing and other service enquiries, call diversion requests, and requests to change a service from being post-paid to pre-paid (and vice versa).

In response, we are proposing to make a determination under subsection 99(1) of the *Telecommunications Act 1997* (the Act) that will apply to all providers of telecommunications services and to all high-risk customer interactions.

A determination will:

Establish obligations that are clear and transparent to all carriage service providers across the whole telecommunications industry.

Require an authorisation process that provides a high level (or ‘silver standard’) of assurance to prevent malicious actors from gaining access to a device and any sensitive information held on it.

Afford the ACMA a broad range of immediately available enforcement powers should there be industry non-compliance, including the use of behavioural remedies such as enforceable undertakings and remedial directions, as well as the possibility of pecuniary penalties.

Be able to be amended to respond to an evolving threat environment in a reasonably short timeframe as compared to other rule making mechanisms available under the Act.

Communications Alliance Limited (Comms Alliance) has recently developed an industry code C666:2021 Existing Customer Authentication (the industry code) and submitted it to the ACMA, for potential registration. The proposed code is supported by a confidential guidance note that would be available to Comms Alliance members to support implementation of the industry code.

The ACMA will consider whether this industry code provides appropriate community safeguards and has met mandatory requirements under the Act. The ACMA notes 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.

The ACMA recognises that it is unusual for it to be consulting on a regulatory instrument while the industry has developed an industry code. However, the ACMA’s priority is to implement the most effective solution to the considerable consumer detriment being experienced.

The ACMA is therefore seeking feedback on its proposed rules in parallel to consideration of the submitted industry code, in order to ensure that enforceable obligations can be established at the earliest possible time. In the interim, we strongly encourage all telecommunications providers to adopt robust customer identity verification processes as a priority to protect their customers while formal processes to make obligations mandatory and enforceable are underway.

We invite submissions on the draft Telecommunications Service Provider (Customer Identity Verification) Determination 2021 (the draft determination) by
**11pm AEDT,** **Wednesday 15 December 2021**.

# Matters for comment

We invite comments on the draft determination, including on the following specific matters:

1. **Effectiveness of the draft determination:**

The draft determination sets out a number of customer identity verification requirements for high-risk customer interactions and ways to deal with the specific circumstances affecting customers in vulnerable customers.

Are these requirements adequate to achieve the objectives of the draft determination to reduce consumer harm and protect the security of high-risk customer interactions?

1. **High-risk customer interactions:**

The draft determination defines high-risk customer interactions.

Will this definition capture all of the interactions targeted by, or vulnerable to, scammers? If not, what are the other interactions?

Are there any specific interactions or class of interactions that should not be considered high-risk, and why?

1. **Multi-factor identity verification processes:**

The draft determination sets out processes for customer identity verification but does not intend to limit providers taking additional or innovative actions.

We are specifically interested in how the proposed processes will work where authorised representative arrangements are in place.

Are there additional examples of *account information, personal information* or *possession-based authenticators* that should be covered by these definitions?

The draft determination imposes a time limit of one day for multi-factor identity verification to be completed using identity documents. Is a time limit required and, if so, is this period appropriate?

1. **Identity verification requirements for customers in vulnerable circumstances:**

The draft determination sets out identity verification requirements for people in vulnerable circumstances, such as emergency and family-violence affected individuals.

Are there additional processes that should be considered?

1. **Implementation:**

The draft determination is proposed to commence on 5 April 2022.

We welcome feedback on the timing of commencement of the determination, including on any staged transitional arrangements that could be considered so that consumer protections are in place as quickly as possible.

In addition to these questions, we welcome comment on any other matters relevant to the provision of consumer protections under the draft determination.

# The draft determination

## Preventing fraud from high-risk customer interactions

Scams over telecommunications networks are a significant problem. Scammers are malicious third-party actors, often operating offshore. They are technologically agile – as they quickly identify and exploit weaknesses in systems and networks.

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.[[2]](#footnote-3)

Evidence indicates that identity fraud over telecommunications networks has primarily occurred in 2 ways:

**Unauthorised mobile porting:** 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

**Unauthorised SIM swap:** 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 device controlled by a scammer.

There is strong evidence that the implementation of the PPV Standard has led to a significant drop in unauthorised mobile porting. Major telecommunications providers have reported a drop of approximately 95% in reported porting fraud cases. The Australian Competition and Consumer Commission (ACCC) has released figures showing an approximate 50% reduction in reported losses in 2020 following the commencement of the PPV Standard in April 2020.[[3]](#footnote-4)

Unfortunately, there is clear evidence that scammers continue to target SIM swap processes, with some data sources indicating ongoing harms have increased. ACMA analysis shows that between January and May this year, more than 80% of mobile number fraud resulted from unauthorised SIM swaps.

We have data from government agencies, telecommunications providers and other bodies that provide a strong indication of about ongoing realised harm. We estimate the average loss per mobile number fraud to be $28,715, and we are aware consumers are likely to under-report fraud to authorities due to embarrassment and reputational issues.

There is also emerging evidence that scammers are targeting other telecommunications customer interactions. For example, scammers have used personal information to facilitate other types of fraud, such as ‘purchasing’ expensive handsets on a customer’s account or gaining full access to customer accounts and payment details. This suggests that if fraud from unauthorised SIM swap is prevented via new obligations, scammers will quickly pivot to target other points of weaknesses.

For these reasons, we are proposing new regulatory obligations in the draft determination to require providers to use multi-factor identity verification for all customer interactions at high risk of fraud. In taking this step, we note that some providers have already introduced multi-factor identity verification arrangements, or are in the process of doing so, under guidance material developed by Comms Alliance. It is demonstrable that providers that have already implemented these processes are experiencing significantly less fraud involving their customers.

We consider that direct regulation through a service provider determination is the appropriate way to address harms from unauthorised SIM swap and other customer interactions because of the:

serious nature of the harms involved

greater range of enforcement powers afforded to the ACMA (including the use of behavioural remedies such as enforceable undertakings and remedial directions, as well as the possibility of pecuniary penalties)

symmetry with the related industry standard to prevent mobile porting fraud (that provides protections against the same bad actors)

ability of the ACMA to amend the instrument quickly and efficiently if required, including due to new areas of attack by scammers.

## Key matters for consideration

### Alignment with existing rules

The draft determination provides regulatory parity with the PPV Standard by imposing 2-step customer identity verification processes on all high-risk customer interactions. To the extent possible, it uses consistent definitions, equivalent objectives and similar identity verification processes.

### Outcomes-based approach

Although not directly responsible for the harms perpetrated by scammers, telecommunications providers are responsible for the security of their networks. As noted above, scammers are malicious third-party actors, often operating offshore, and are able to quickly identify and exploit weaknesses in networks and processes.

Telecommunications providers differ in size, scale of operation and interaction with customers.

For these reasons, the draft determination has been drafted to meet the required objectives, while leaving it open to providers to determine which processes are applicable, and how they will be implemented. This approach will promote innovation and adaptation in the medium to longer term, while also helping to keep specific and/or sensitive information relevant to particular providers’ solutions out of the public domain and hands of bad actors.

In developing the draft determination, we have considered the existing customer identity verification processes that many providers have already implemented or are in the process of implementing. These are contained in the industry code developed by Comms Alliance.[[4]](#footnote-5)

### Multi-factor identity verification

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. When implemented correctly, it can be a highly effective strategy to mitigate harm, particularly where remote authentication is required.

The Australian Cyber Security Centre provides guidance on Implementing Multi-Factor Authentication[[5]](#footnote-6) that is relevant to its use by telecommunications providers:

When multi-factor authentication is implemented correctly, it is significantly more difficult for an adversary to steal a complete set of credentials as the user has to prove they have physical access to a second factor that either they have (e.g., a physical token, smartcard or software certificate) or are (e.g., a fingerprint or iris scan). When implementing multi-factor authentication, it is essential that it is done so correctly to minimise security vulnerabilities and to avoid a false sense of security that could leave a network vulnerable.

In addition, the draft determination reflects better industry practice to combat scammers, by requiring providers to inform the customer:

that a high-risk interaction has been instigated

the nature of the high-risk interaction

what the customer should do if they did not authorise the transaction.

### Identity protection and security risk

The Australian Government’s National Identity Security Strategy and National Identity Proofing Guidelines (the guidelines)[[6]](#footnote-7) offer guidance about the preservation and protection of a person’s identity as a ‘key concern and a right of all Australians’.

While not containing mandatory obligations for the private sector, the guidelines provide better practice that we have considered in drafting the draft determination.

Relevant guidance includes identity proofing objectives and levels of assurance for remote (e.g., online or via phone) or local (in-person) processes.

The guidelines indicate a high (or ‘silver standard’) level of assurance is desirable for remote and local transactions with:

[S]erious consequences associated with fraudulent registration, such as allowing access to sensitive information, systems or people, including those of organisations other than that which undertook the initial identity proofing. Examples include issuance of documents and credentials used as secondary evidence of identity in the community.

Evidence is required to confirm the linkage between the identity and the person claiming the identity. The guidelines state it may be obtained through the approaches set out in Table 1 below.

Confirming identity at a silver standard

|  |
| --- |
| Approaches |
| Manual/visual comparison of a person’s face against a photograph on a primary piece of evidence (either remotely or in person). |
| Verification of a biometric[[7]](#footnote-8) template collected at registration (either remotely or in person) against a biometric template held by an authoritative source. |
| Knowledge-based authentication (if questions are derived from multiple authoritative sources, do not use publicly available information, are randomised and a time limit is set for answering the questions or other equivalent practices are used). |

### Future proofing for digital identity verification

The government has recently concluded consultation on the *Trusted Digital Identity Bill 2021 (Exposure Draft)[[8]](#footnote-9)* to establish permanent oversight and governance structures for the government Digital Identity System and enshrine in law important privacy and consumer protections.

If passed, the legislation will:

enable the expansion of the Australian Government Digital Identity System, specifically to enable greater participation by state and territory governments and the private sector

enshrine in law various privacy and consumer protections, so that Australians can have confidence in the System and know that their personal information is safe and secure

establish permanent governance arrangements and a strong regulatory regime.

Consistent with the PPV Standard, the draft determination includes government online verification services as a possible element of multi-factor identity verification where standard forms of verification cannot be used.

### Practicable, robust and technically feasible processes

The identity verification processes set out in the draft determination are largely drawn from those outlined in the PPV Standard and from examples of industry better practice.

### Additional protections for all customers

The draft determination also contains a number of additional protections for customers, which we identified where needed from our enforcement of the PPV Standard and/or which we consider reflect industry better practice.

Complaint and report data about fraud indicates that some customers have been a victim of porting fraud on several occasions, sometimes only days apart. Other intelligence suggests that once a customer’s identity has been compromised, they can be repeatedly targeted, for example, where their primary identity documents have been stolen or otherwise obtained.

To mitigate these harms, some providers are allowing ‘at-risk’ flags to be placed on accounts, in consultation with, or at the request of, customers. Reflecting this industry better practice, the draft determination requires providers to provide additional levels of protection if requested. It also requires providers to offer customers additional levels of protection if they are made aware that the customer’s identity has been compromised (for example, via a fraud attempt involving the customer’s account).

In addition to this, the draft determination requires providers’ in-store staff or agents who handle specified identity documents to have undergone relevant fraud training. This recognises identity documents themselves can be subject to fraud.

### Protections for customers in vulnerable circumstances

We have considered policies and processes from the telecommunications and other industries to cater for customers who may be in vulnerable circumstances and therefore cannot access a device, service or documents required to complete the multifactor identity verification processes.

The approach seeks to balance the need to provide additional flexibility for individuals in vulnerable circumstances with the need to limit the ability of scammers to exploit exceptions to multi-factor identity verification requirements.

The outcomes-based approach, which leaves it open to providers to determine which processes are applicable, will also enable providers to tailor multi-factor identity verification requirements to suit certain types of customers. For example, providers may give customers the choice to receive a unique verification code by email rather than SMS message and must do so if specifically requested to.

Additionally, as noted above, the draft determination includes requirements that providers give additional protections to all customers at their request, allowing for greater protection for customers where the security of their personal information is of particular concern.

### Costs and administrative burden

As noted above, the processes set out in the draft determination are largely drawn from industry practices that have been implemented to comply with the PPV Standard or current industry better practice.

We have also considered the costs of customer identity verification processes on customers. Consistent with the PPV Standard, each provider will bear its own costs and should not charge customers a fee for the customer identity verification processes. This will ensure all customers (including customers with zero credit on
pre-paid mobile services) can send back unique codes to allow providers to verify their identity.

**Records keeping**

In conducting compliance activities relating to existing customer authentication rules under the PPV Standard, and collating data which informed the draft determination, we have become aware that data held by providers about fraud is often inconsistent with data held by financial institutions about telecommunications-related fraud.

To assist in compliance and enforcement activities under the new rules and to aid understanding of whether further regulatory reform is required in relation to bad actors targeting or circumventing new measures, we are of the view that records should be kept demonstrating compliance with the determination for a minimum of 12 months after a transaction.

These records may further assist providers to meet proposed obligations about flagging at-risk customers; when assessments have been made relating to customers in vulnerable circumstances; and broader privacy obligations in relation to the use of personal information for processes mandated under regulation.

### Provision of education and safeguard information

Most industry and consumer submissions to the ACMA’s Scam Technology Project[[9]](#footnote-10) indicated strong views that consumer education and empowerment was a key component to reducing the harms perpetrated by scammers.

Accordingly, and again consistently with the PPV Standard, the draft determination specifies that providers must advise customers that multi-factor customer identity verification will be required for all high-risk interactions. In addition, providers must provide customers with information about who to contact if they suspect their telecommunications service or account has been subject to fraud.

The draft determination requires this information to be provided directly to customers, and on providers’ websites.

# Invitation to comment

## Making a submission

The ACMA invites comments on the issues set out in this paper.

[Online submissions](https://www.acma.gov.au/have-your-say) can be made via the comment function or by uploading a document. Submissions in Microsoft Word or Rich Text Format are preferred.

Submissions by post can be sent to:

The Manager
Strategy and Projects Section
Australian Communications and Media Authority
Law Courts
Melbourne VIC 8010

The closing date for submissions is **11pm AEDT,** **Wednesday 15 December 2021**.

Consultation enquiries can be emailed to unsolicitedcommsprojects@acma.gov.au.

#### Publication of submissions

The ACMA publishes submissions on our website, including personal information (such as names and contact details), except for information that you have claimed (and we have accepted) is confidential.

Confidential information will not be published or otherwise released unless required or authorised by law.

In this case, the ACMA notes that submissions may contain sensitive information that it is not in the public interest to publish.

#### Privacy

View information about our policy on the publication of submissions, including collection of personal information during consultation and how we handle that information.

Information on the *Privacy Act 1988* and the ACMA’s privacy policy (including how to access or correct personal information, how to make a privacy complaint and how we will deal with the complaint) is available at [acma.gov.au/privacypolicy](http://www.acma.gov.au/privacypolicy).

1. 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. [↑](#footnote-ref-2)
2. Identity Theft Resource Centre, 2018, [*The Aftermath – the non-economic impacts of identity theft*](https://www.idtheftcenter.org/wp-content/uploads/2018/09/ITRC_Aftermath-2018_Web_FINAL.pdf), viewed 16 October 2021. [↑](#footnote-ref-3)
3. ACCC, [Targeting scams: Report of the ACCC on scam activity 2020](https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2020), viewed 16 October 2021. [↑](#footnote-ref-4)
4. Communications Alliance, 2021, [*Draft Existing Customer Authentication Code 2021*](https://commsalliance.com.au/__data/assets/pdf_file/0006/78054/Cust-Authentication_2021_Public-Comment.pdf), viewed 23 September 2021. [↑](#footnote-ref-5)
5. ACSC, 2021,[*Implementing Multi-Factor Authentication,*](https://www.cyber.gov.au/sites/default/files/2021-10/PROTECT%20-%20Implementing%20Multi-Factor%20Authentication%20%28October%202021%29.pdf) viewed 12 October 2021. [↑](#footnote-ref-6)
6. Department of Home Affairs, 2016, [*National Identity Proofing Guidelines*](https://www.homeaffairs.gov.au/criminal-justice/files/national-identity-proofing-guidelines.pdf)*,* viewed 23 September 2021. [↑](#footnote-ref-7)
7. The guidelines define ‘biometric information’ as information about any measurable biological or behavioural characteristics of an individual that can be used to identify the individual or verify the identity of the individual, such as face, fingerprints and voice. [↑](#footnote-ref-8)
8. Digital Transformation Agency, [Draft legislation for Australian Government Digital Identity System](https://www.dta.gov.au/news/draft-legislation-australian-government-digital-identity-system), viewed 7 October 2021. [↑](#footnote-ref-9)
9. ACMA, 2019, [Scam Technology Project](https://www.acma.gov.au/scam-technology-project), viewed 23 September 2021. [↑](#footnote-ref-10)