Proposal to vary the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022

Consultation paper

DECEMBER 2024

Canberra

Level 3
40 Cameron Avenue
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
F +61 2 9334 7799

Copyright notice



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

Except for the Commonwealth Coat 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.

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.

We request attribution as © Commonwealth of Australia (Australian Communications and Media Authority) 2024.

[Executive summary 1](#_Toc184298400)

[Proposed variations 2](#_Toc184298401)

[Passkeys 2](#_Toc184298402)

[Unique verification code or secure hyperlink 2](#_Toc184298403)

[Government-accredited digital identity service 3](#_Toc184298404)

[Exceptions to sending notifications about high-risk customer transactions 4](#_Toc184298405)

[Identity authentication process using visual comparison to documents 5](#_Toc184298406)

[Government death notification system 5](#_Toc184298407)

[Record keeping 5](#_Toc184298408)

[Material and supporting evidence 5](#_Toc184298409)

[New sections 6](#_Toc184298410)

[Protecting records 6](#_Toc184298411)

[Overview of proposed guidance 8](#_Toc184298412)

[Invitation to comment 10](#_Toc184298413)

[Making a submission 10](#_Toc184298414)

[Publication of submissions 10](#_Toc184298415)

[Privacy 10](#_Toc184298416)

Executive summary

The Australian Communications and Media Authority (ACMA) made the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 (Determination) in April 2022 to reduce harms associated with unauthorised high-risk customer transactions affecting telecommunications services.

The Determination was made under subsection 99(1) of the *Telecommunications Act 1997*. It applies to carriage service providers (CSPs) of telecommunication services and to high-risk customer interactions, except where a customer is an account-managed customer or an integrated customer. The Determination has:

* established obligations that are clear and transparent to all CSPs across the telecommunications industry
* implemented an authorisation process that provides a high level of assurance to prevent malicious actors from gaining access to a device and any sensitive information held on it
* afforded the ACMA a broad range of immediately available enforcement powers for industry non-compliance, including the use of behavioural remedies such as enforceable undertakings, as well as pecuniary penalties.

There is strong evidence that the implementation of the Determination has led to a significant drop in fraudulent high-risk customer transactions (for example, reports available to the ACMA about mobile number fraud decreased by nearly 70% between 2021 and 2023) and that it continues to provide critical protections to consumers.

We are proposing to vary the instrument to support innovation, strengthen the requirements to protect vulnerable people and provide clarity to the telecommunications sector.

We have received feedback from industry and conducted targeted initial engagement with some telcos and consumer bodies to inform the proposed variations, which will not diminish the current protections.

Subject to consideration of submissions, and following the variation of the Determination, we will develop guidance for industry on best practices and compliance obligations for the varied instrument. While this guidance will be informed by any variations to the Determination, the key areas we expect to cover are set out in the *Overview of proposed guidance* section of this paper.

We welcome submissions on the proposed variations to the Determination by midday (AEST), **Friday** **14 February 2025.**

# Proposed variations

We invite comment on the following proposed variations to the Determination. A draft of the proposed Determination is available alongside this paper on the ACMA website.

**Multi-factor Authentication Requirements**

### Passkeys

We propose including use of a passkey as an additional alternative identity authentication process at subsection 9(1). A passkey enables a user to access the security features on a phone, computer, or tablet to sign in to apps and websites.[[1]](#footnote-2)

**Issue for comment 1:**

1. Do you agree or disagree with including use of a passkey as an alternative first-factor identity authentication process?
2. Does it pose any security or fraud risks? If so, please describe these in detail.
3. Is the definition of passkey in the draft Determination appropriate? Do you have any alternate suggestions?

### Unique verification code or secure hyperlink

We propose updating paragraph 9(3)(c)(i) to allow a unique verification code or secure hyperlink to be sent via SMS message to either:

1. the mobile service number that is listed on the account as the contact number for the customer, or
2. where there is no mobile service number listed on the account as the contact number for the customer – the mobile service number of the customer.

In some cases, we understand that CSPs may not have a listed number on an account, however, will have the service number. N.B. in either case, the number is directly associated with the account and would not open avenues for fraud.

Paragraph (b) above is intended to permit the sending of a unique verification code or secure hyperlink by SMS in circumstances where the customer has listed a landline number as the contact number for the customer (that is, a number to which an SMS cannot be sent) or where the customer has not listed any number as the contact number for the customer. In such circumstances, a CSP will be permitted to send the relevant SMS message to the mobile service number of the customer.

**Issue for comment 2:**

1. Do you agree with allowing a unique verification code or secure hyperlink to be sent via SMS message to the mobile service number of the customer?
2. Are there alternative methods that could be used? If so, please provide details.
3. Are there any concerns for persons in vulnerable circumstances?

### Government-accredited digital identity service

We are proposing to update the identity authentication processes at subsection 9(3) to include government-accredited digital identity services as a primary option for CSPs to authenticate customers.

The government is developing a legislated accreditation scheme for entities that provide digital identification (ID) services (commencing December 2024) and has established a Digital ID System[[2]](#footnote-3) to support the use of digital ID services as an easier and more secure way to verify ID.

The proposed variation sets out government-accredited digital ID services as a primary option, rather than a possible authentication method after other methods have been attempted in the current instrument.

We have considered the government’s National Strategy for Identity Resilience (the Strategy for ID Resilience)[[3]](#footnote-4) in drafting the proposed changes. The proposed change is consistent with the Strategy for ID Resilience, which contains shared principles including supporting use of digital ID systems and credentials so that Australians can access services and reduce the amount of information they share.

**Issue for comment 3:**

1. Do you agree with including use of a government accredited digital identity services as the primary option to authenticate customers? If not, please explain why.
2. Are there any concerns for persons in vulnerable circumstances?

**Use of biometric data and record keeping**

Biometric information is considered sensitive information under the [*Privacy Act 1988*](https://www.legislation.gov.au/C2004A03712/latest/text), which places additional obligations on organisations. The use of biometric information[[4]](#footnote-5)may be high-risk as, unlike other forms of ID (for example, a Medicare card), biometric information cannot be replaced if it is subject to identity theft or is disclosed in a data breach.

Use of biometrics is currently an identity authentication process at subsection 9(3) of the Determination. Due to the inherent risks involved to consumers, we are proposing the use of biometrics as a possible authentication method only where the primary methods and secondary methods cannot be used. We also propose including specific consent and record-keeping requirements under section 10 when using biometrics.

We have considered the Strategy for ID Resilience and guidance on facial recognition technology from the Office of the Australian Information Commissioner (OAIC)[[5]](#footnote-6) in drafting the proposed variation. The proposed changes are consistent with the principles in the strategy to obtain consent, protect personal privacy and secure data when using biometrics for identity verification.[[6]](#footnote-7) The proposed changes are so that the use of biometrics only occurs when verification cannot be reasonably achieved through less privacy-intrusive means.

Subject to consideration of submissions, we remain open to entirely removing biometrics as an authentication method. If provisions relating to biometrics remain in the varied Determination, the ACMA anticipates providing additional guidance on its use, including in relation to conducting Privacy Impact Assessments.

**Issue for comment 4:**

1. Do you agree with changing the use of biometric data from a primary method of authentication to being a *possible* authentication method?
2. Are there any concerns for persons in vulnerable circumstances?
3. Are there alternative methods that could be used? If so, please provide details

**We are also interested in the following information from CSPs:**

1. If you use biometric data, how are you currently using it? Please provide any details on how these changes will impact any current use of biometric information?
2. What kind of consent (explicit or implied) is currently being sought or used from requesting persons? How is it being obtained?
3. Is consent obtained once or each time biometric information is used?
4. Do you outsource biometric information processing? If so, what assurances are in place for third parties to meet privacy requirements?

### Exceptions to sending notifications about high-risk customer transactions

We are proposing that the exceptions to sending notifications about high-risk customer transactions be expanded to include the customer’s authorised representative. Currently, the exceptions under subsections 10(8), 11(6) and 12(6) only apply where the CSP has reasonable grounds to believe the customer is affected by domestic or family violence and the customer has requested that the notification is not sent.

We are also proposing providing clarity about when notifications must occur where a high-risk customer transaction has been requested by an unlisted authorised representative, and a CSP is satisfied that a relevant person is subject to advice under a government death notification system. To inform final drafting, we encourage submissions from CSPs about who may be contacted where an unlisted authorised representative is involved in such circumstances.

This proposed change intends to better support people who may be experiencing domestic or family violence, and those who have suffered a bereavement.

**Issue for comment 5:**

1. Do you agree with expanding the exceptions to sending notifications about high-risk customer transactions to include the customer’s authorised representative?
2. Do you agree to providing clarity about when exceptions apply to notifications where an unlisted authorised representative is requesting a high-risk transaction in relation to a person who is deceased? Would such an exception pose risks for customers or customers’ authorised representatives?
3. In cases where an unlisted authorised representative is requesting a high-risk transaction in relation to someone who is deceased, who are the relevant people connected with an account that a CSP would then deal with about that account?
4. Are there alternative approaches that could be used? If so, please provide details.

### Identity authentication process using visual comparison to documents

Schedule 1 of the Determination outlines the identity authentication process for undertaking a visual comparison of the requesting person’s face against category A and category B documents.

Clause 4 of Schedule 1 specifically relates to the process used for authenticating under paragraph 9(3)(e). Clause 4 requires CSPs to undertake the visual comparison either in person or by live audio-visual link. The Determination does not provide an alternative at Clause 4 where both options are not suitable.

We may consider a variation to these rules if there is evidence to support that an alternative process will support customers and doesn’t expose them to additional risk of fraud.

**Issue for comment 6:**

**We are interested in the following information from CSPs**

1. Do you encounter issues authenticating customers under Clause 4 of Schedule 1? If so, please provide details.
2. Are there alternative approaches that could be used for customers with limited digital literacy who cannot access a CSP’s store? If so, please provide details.

### Government death notification system

We propose amending subsection 12(2) to include express mention of a government death notification system[[7]](#footnote-8) as an example of documentary evidence that a CSP can use to satisfy itself that a requesting person is an unlisted authorised representative.

The proposed change intends to enable CSPs to provide clarity to telcos to better support unlisted authorised representatives in bereavement circumstances. ​

**Issue for comment 7:**

1. Do you agree with including a government death notification system as an example of documentary evidence?
2. Are there alternative approaches that could be used? If so, please provide details.

## Record keeping

### Material and supporting evidence

We are proposing to clarify the record-keeping requirements at paragraphs 11(3)(c) and 12(3)(b) to specify that it applies to the *type* of material or supporting evidence provided to CSPs. That is, a CSP will not be required to keep the actual material or supporting evidence provided by the requesting person; they will just be required to keep a record of the *type* of material or supporting evidence that was provided.

For example, a CSP that sights an enduring power of attorney as part of an identity authentication method is not required to store a copy of the document or any information contained on the document. The CSP would only be required to keep a record of the fact that they had sighted the enduring power of attorney.

This proposed change is to add clarity about the records that CSPs must retain to demonstrate compliance and any need to store sensitive and personal information. The proposed change is consistent with the paragraph 17(1)(a) requirement for records to be kept, demonstrating compliance with the Determination and with the shared principles in the Strategy for ID Resilience[[8]](#footnote-9) of less data collection and retention.

**Issue for comment 8:**

1. Do you agree with clarifying the record-keeping requirements to keep a record of the type of material or supporting evidence provided, rather than the actual material or evidence?
2. Are there alternative approaches that could be used? If so, please provide details.
3. Are there any concerns in relation to persons in vulnerable circumstances?

We propose varying section 17 to clarify that material or supporting information provided under paragraph 11(1)(b) and subsection 12(2) is only retained for the period required to complete the authentication process and is securely destroyed thereafter.

**Issue for comment 9:**

1. Do you agree with clarifying that material or supporting information provided should only be used to complete authentication and be securely destroyed after?
2. Are there alternative approaches that could be used? If so, please provide details.
3. Are there any concerns for persons in vulnerable circumstances?

## New sections

**General matters - Privacy**

We propose a variation to include privacy obligations where a CSP is not subject to the requirements of the *Privacy Act 1988*. This will help ensure that personal information is collected in connection with identity authentication is not disclosed to a third party except in specific circumstances, and that the information is used, stored, or disclosed, and disposed of, or destroyed in a secure manner.

**Issue for comment 10:**

1. Do you agree with including privacy obligations if a CSP is not subject to the requirements of the Privacy Act?

### Protecting records

We propose a variation to include general obligations for record security under Part 6 – Record Keeping. This proposed section intends to protect customers’ records by, in effect, requiring CSPs to have effective processes and systems in place to secure records relating to identity authentication and to securely dispose of records when they are no longer needed. We expect that CSPs will already have such processes in place, and that this will promote consistency and compliance across the sector.

**Issue for comment 11:**

1. Do you agree with including obligations for record security?

**Costs and impacts**

We encourage detailed submissions from telecommunications providers on any regulatory benefit and/or burden associated with the variations.

**Issue for comment 12:**

1. What are the likely costs and impacts of implementation of these variations?

We welcome detailed information about any issues and costs against each proposed amendment, as applicable. Information may be provided to the ACMA confidentially, noting this must be made clear in the submission. Information about initial benefits/impacts and subsequent benefits/impacts is also welcome.

# Overview of Proposed Guidance

Feedback on the current Determination from parts of industry has indicated that some CSPs are either unclear about their obligations and/or have adopted specific compliance processes that are not warranted.

Once a revised Determination is finalised, we propose to provide guidance, including on the key matters set out below.

**Table 1: Proposed key areas for guidance to industry**

| **Topic** | **Issue**  | **Nature of proposed guidance** |
| --- | --- | --- |
| Use of biometrics  | There is no consistency to the way biometrics are currently used across industry and privacy risks may be unaddressed  | * When biometrics can be used
* What constitutes ‘free and informed consent’
* Considering Privacy Impact Assessments and implementing outcomes to minimise data privacy risks
* What records should be retained
 |
| Privacy  | CSPs have inconsistent practices and understandings about obligations that relate to record-keeping and privacy  | * Expectations that CSPs meet obligations by only retaining details that are accurate and relevant to compliance with the Determination and Privacy Act
* Expectations for CSPs that are not subject to the Privacy Act 1988
 |
| Customer safety training  | CSPs have inconsistent practices and consumer stakeholders have raised that this type of training can be important to appropriately support people experiencing vulnerability  | * That key employees have training in recognising, and responding to people experiencing domestic and family violence, including elder abuse, and regarding trauma-informed principles
 |
| Use of government death notification system  | At least one CSP has considered that use of the government death notification system to inform customer notification obligations is not enabled by the Determination  At least one CSP indicated it may be using the personalised names of deceased persons in notifications regarding the service  | * That the Determination does not prevent use of the government death notification system
* That the Determination does not require personalised communications
* How the system may be used
 |
| What constitutes a high-risk customer transaction  | At least one CSP has considered that minor international roaming charges would meet the definition of a high-risk customer transaction Some CSPs have raised concerns that certain eSIM transfers by customers that are managed on their devices (without need to engage with a CSP) may be captured by the definition of a high-risk transaction  | * That such roaming charges are not ongoing OR large one-off, and therefore do not meet the definition of a high-risk customer transaction
* That in cases where the CSP is not involved in the interaction, such as an eSIM, it does not constitute a high-risk customer transaction for the purposes of the Determination (as in this case, there is no request to the telco from the customer or the authorised representative)
 |
| People in vulnerable circumstances  | Some CSPs have incorrectly interpreted provisions about assessing a person in vulnerable circumstances as being restrictive  | * Explaining that the arrangements are not exclusive nor exhaustive, and the provisions may include where someone may have lost their telecommunications service
 |
| Use of MFA in cases where the customer is unable to use a particular method  | At least one CSP has suggested it would like to rely on previous customer interactions in some cases as a part of MFA, as opposed to using other available methods for MFA  | * The expectation that CSPs would attempt another method of MFA where an initial method is not available
 |
| Passive authentication of identity   | CSPs are unclear about any opportunities permitted for passive authentication of identity  | * The Determination does not prevent passive authentication
* That ‘direct and immediate access’ requirements are not exclusive or exhaustive
* Passive authentication will need to consider what the considerations are for each of the potential types and how these may work in practice to ensure they do not expose customers to risk
 |

# Invitation to comment

## Making a submission

We invite comments on the issues set out in this consultation paper.

* [Online submissions](https://www.acma.gov.au/have-your-say) can be made by uploading a document. Submissions in PDF, Microsoft Word or Rich Text Format are preferred.
* Submissions by post can be sent to:

The Executive Manager
Unsolicited Communications & Scams Branch
Australian Communications and Media Authority
PO Box 13112
Law Courts
Melbourne VIC 8010

The closing date for submissions is midday (AEST), **Friday 14 February 2025**.

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

### Publication of submissions

We publish 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.

### Privacy

View information about our policy on the [publication of submissions](https://www.acma.gov.au/publication-submissions), including collection of personal information during consultation and how we handle that information.

Information on the *Privacy Act 1988*, how to access or correct personal information, how to make a privacy complaint and how we will deal with any complaints, is available in our [privacy policy](https://www.acma.gov.au/privacy-policy).

1. Services Australia, [Use Passkeys](https://my.gov.au/en/about/help/mygov-website/sign-in-to-mygov/use-passkeys), accessed 28 October 2024. [↑](#footnote-ref-2)
2. Department of Finance, [*Australia’s Digital ID System*](https://www.digitalidsystem.gov.au/), [www.digitalidsystem.gov.au](http://www.digitalidsystem.gov.au), accessed 22 October 2024. [↑](#footnote-ref-3)
3. Attorney-General’s Department, [*National Strategy for Identity Resilience*](https://www.ag.gov.au/sites/default/files/2023-08/national-strategy_for-identity-resilience.pdf), Attorney-General’s department website, 2023, accessed 23 October 2024 [↑](#footnote-ref-4)
4. The Strategy for ID Resilience defines biometric information as information about any measurable biological or behavioural characteristics of a natural person that can be used to identify them or verify their identity, such as face, fingerprints and voice. Biometric information includes biometric templates. [↑](#footnote-ref-5)
5. Office of the Australian Information Commissioner (OAIC), [*Facial recognition technology: a guide to assessing the privacy risks*](https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/organisations/facial-recognition-technology-a-guide-to-assessing-the-privacy-risks), OAIC website, 2024, accessed 29 November 2024. [↑](#footnote-ref-6)
6. Attorney General’s Department, *National Strategy for Identity Resilience*. [↑](#footnote-ref-7)
7. NSW Department of Customer Service, [*Australian Death Notification Service*](https://deathnotification.gov.au/), Australian Death Notification Service website, 2021, accessed 18 November 2024. [↑](#footnote-ref-8)
8. Attorney General’s Department, *National Strategy for Identity Resilience*. [↑](#footnote-ref-9)