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

13 February 2025

Recommendations

This submission recommends the ACMA:

- Ensure multi-factor authentication options are designed to accommodate the diverse needs and circumstances of individual consumers.
- Facilitate timely and accessible customer service support for identity verification concerns and cases of suspected scams or fraudulent activity.

About this submission

The Australian Communications Consumer Action Network (**ACCAN**) is pleased to provide this submission to the Australian Communications and Media Authority (**ACMA**) on the proposal to vary the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 (**the Determination**).

ACCAN recommends that the proposed changes to the Determination prioritise meeting diverse consumer needs, balancing fraud prevention with easy account access and management. Additionally, customer service for identity verification and scam-related issues should be timely and accessible to ensure consumers receive adequate support.[1]

[1] See, ACCAN, *Proposal to make the Telecommunications Service Provider (Customer Identity Verification) Determination 2021* (Policy Submission, ACMA, 15 December 2021).

Contents

Australian Communications Consumer Action Network

Australian Communications Consumer Action Network

ACCAN is the peak national consumer advocacy organisation for communications working to achieve trusted, accessible, inclusive, affordable and available communications and digital services for all Australians.

Introduction

ACCAN welcomes the proposed variations to the Determination, which aim to enhance the security of communications services and better protect consumers from identity fraud.

In our previous submission, ACCAN acknowledged the challenge of balancing improved security and fraud prevention with ensuring consumers are not unfairly excluded from accessing or managing their accounts.[2] This balance is particularly critical for people experiencing vulnerability or with limited digital skills, who are disproportionately impacted by fraud while also facing greater challenges navigating rigid or automated identification authentication processes.

To address these issues, ACCAN reiterates its recommendations that the Determination requires Communications Service Providers (**CSPs**) to:

- Ensure multi-factor authentication methods meet the diverse needs of individual consumers.[3]
- Provide timely, accessible, and high-quality customer service to address ID verification issues and suspected scams or fraudulent activity.[4]

These measures will help ensure that the ACMA supports robust fraud prevention while remaining inclusive and responsive to the needs of all consumers.

ACCAN's response to the proposed variations

Multi-factor Authentication Requirements

Issue for comment 1: Passkeys

ACCAN supports the inclusion of passkeys as an alternative identity authentication method under subsection 9(1) of the Determination. However, we recommend Section 6 should remove the reference to biometrics in the definition of passkeys (Changes in ~~strikethrough~~).

> ***passkey*** means a security feature of a mobile phone, computer or tablet used to sign in to mobile applications and websites, including using:
>
> ~~(a) biometrics, such as fingerprint or facial recognition;~~
>
> (b) a personal identification number or swipe pattern; or
>
> (c) a physical security key.

ACCAN is concerned about the potential risks associated with relying on biometrics as part of the passkey system. In the event of a widespread cyberattack or data breach targeting biometric systems, consumers could face serious challenges, including the inability to securely re-authenticate their identities.

[2] See, ACCAN, *Proposal to make the Telecommunications Service Provider (Customer Identity Verification) Determination 2021* (Policy Submission, ACMA, 15 December 2021).
[3] Ibid 5.
[4] Ibid 6.

Additionally, we are worried about the challenges and risks that passkeys may pose for consumers in vulnerable situations. Since passkeys are cryptographically linked to the original enrolment device, their effectiveness relies on the security of that device and the consumer's access to it. For instance, victim-survivors of Domestic and Family Violence (**DFV**) may encounter significant barriers to accessing their accounts if they cannot safely use their personal devices or if they share devices with perpetrators.

Despite these challenges, passkeys have the potential to enhance security and reduce consumer frustration. By addressing these risks and ensuring flexible implementation, passkeys can provide a secure, convenient, and inclusive authentication method that protects consumers while maintaining accessibility.

Issue for comment 2: Unique verification code or secure hyperlink

While sending unique verification codes via SMS is a widely accepted method of multi-factor authentication, ACCAN has serious concerns about using secure hyperlinks in SMS messages.

Cybersecurity experts consistently warn consumers against clicking on hyperlinks sent via SMS, as this is a common tactic used by scammers to impersonate legitimate services and conduct phishing attacks.[5] Encouraging interaction with these links can confuse consumers and undermine established security practices, increasing the risk of exposure to scams.

Additionally, some vulnerable consumers may not have access to the phone number linked to their account when a verification code or hyperlink is sent. This is especially relevant for victim-survivors of DFV or individuals who have lost their devices.

While the technical implementation of secure hyperlinks may be sound, the risks associated with encouraging habitual interaction with a known scam vector outweigh potential benefits over using verification codes. Verification codes, which require consumers to manually enter the code, are a more secure and practical alternative that avoids the risks tied to hyperlinks. ACCAN therefore recommends:

- Focusing on unique verification codes, instead of a secure hyperlink, in SMS messages.
- Offering clear education on identifying legitimate communications from service providers to boost consumer confidence without increasing scam exposure.

By focusing on methods like unique verification codes, we can support effective multi-factor authentication while protecting consumers from cyberattacks and addressing the needs of vulnerable individuals.

Issue for comment 3: Government-accredited digital identity service

ACCAN does not support updating subsection 9(3) of the Determination to include government-accredited digital identity services as the primary method for customer authentication by CSPs. While these services may offer a secure and streamlined option for some consumers, making them

[5] Australian Government, 'Text or SMS scams', *ScamWatch* (Web Page, n.d.) <https://www.scamwatch.gov.au/types-of-scams/text-or-sms-scams>.

the primary method risks excluding vulnerable consumers who may be unable or unwilling to create and use a government-accredited digital identity service.

Furthermore, the Australian Government's digital identity system is still in its early stages, with uncertainty surrounding its security, reliability, and uptake among the broader population. Relying on this system as a primary authentication mechanism could inadvertently alienate consumers who are not yet familiar or comfortable with it.

Issue for comment 4: Use of biometric data and record keeping

ACCAN does not support the Determination using biometric data as an authentication method.

For example, advancements in artificial intelligence pose a threat to authentication systems that rely on auditory or visual cues for verification.[6] These security and privacy concerns justify the need to reduce reliance on biometrics as an authentication method.

Issue for comment 5: Exceptions to sending notifications about high-risk customer transactions

ACCAN supports expanding exceptions for sending notifications about high-risk customer transactions to include authorised representatives affected by DFV and should align with the upcoming Industry Standard on DFV.[7] We also recommend that the ACMA ensure timely and accessible customer service support for identity verification and fraud concerns.

However, we seek clarification on exceptions for sending notifications involving unlisted authorised representatives, as these could compromise consumer safety and privacy, particularly for vulnerable individuals. To address this, CSPs should implement strict verification processes and require documentation before processing high-risk transactions.

In cases where unlisted authorised representatives request transactions for deceased individuals, CSPs should consult relevant parties, such as the estate's executor or legal guardians. Decisions should prioritise the designated power of attorney. Without proper safeguards, these situations pose significant risks, so clear protocols must be established for verifying identity and legal standing.

Issue for comment 6: Identity authentication process using visual comparison to documents

ACCAN has no comments.

Issue for comment 7: Government death notification system

ACCAN supports amending subsection 12(2) to include the government death notification system as an example of documentary evidence that a CSP can use to satisfy that a requesting person is an unlisted authorised representative. However, ACCAN recommends initiating this process after the CSP has attempted to contact the listed authorised representative and the account holder.

---

[6] Jennifer Tang, Tiffany Saade and Steve Kelly, *The Implications of Artificial Intelligence in Cybersecurity: Shifting the Offense-Defense Balance* (Report, The Institute for Security and Technology, October 2024) 10.
[7] See, Minister for Communications and Minister for Social Services, 'Better protections for telco customers experiencing domestic and family violence' (Media Release, 8 October 2024).

Record Keeping

Issue for comment 8: Material and supporting evidence

ACCAN supports the clarification of record-keeping requirements to ensure that only the type of material or supporting evidence provided is recorded, rather than retaining the actual material or evidence. This approach balances effective record-keeping with consumer privacy and security.

Issue for comment 9: Materials and supporting evidence

ACCAN supports clarifying section 17, stating that materials and supporting information should only be used for authentication purposes and must be securely destroyed afterwards.

New Sections

Issue for comment 10: General matters – privacy

ACCAN supports the proposed variation to include privacy obligations where a CSP is not subject to the requirements of the *Privacy Act 1998* (Cth). Section 16 of the Determination will help ensure consistent privacy protections across all CSPs, which is essential for safeguarding consumer data.

Issue for comment 11: Protecting records

ACCAN supports the inclusion of obligations for record security within Part 6 – Record Keeping. Clearly defining requirements for protecting records is crucial for safeguarding consumer information and maintaining trust.

Issue for comment 12: Costs and impacts

ACCAN has no comments.

Conclusion

ACCAN welcomes the proposed variations to the Determination, which aim to enhance security and protect communications consumers from identity fraud. These measures will ensure the Determination supports effective fraud prevention while remaining inclusive and consumer focused.

We thank the ACMA for the opportunity to comment on the Determination. Should you wish to discuss any of the issues raised in this submission further, please do not hesitate to contact me at amelia.radke@accan.org.au.

Yours sincerely,

Dr Amelia Radke
Senior Policy Adviser

The Australian Communications Consumer Action Network (ACCAN) is Australia's peak communication consumer organisation. The operation of ACCAN is made possible by funding provided by the Commonwealth of Australia under section 593 of the Telecommunications Act 1997. This funding is recovered from charges on telecommunications carriers. ACCAN is committed to reconciliation that acknowledges Australia's past and values the unique culture and heritage of Aboriginal and Torres Strait Islander peoples. Read our RAP.