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

Submission by the Australian Communications Consumer Action Network to the Australian Communications and Media Authority

15 December 2021

Australian Communications Consumer Action Network (ACCAN)
Australia's peak telecommunications consumer organisation

PO Box A1158, Sydney South NSW 1235
Tel: (02) 9288 4000 | Contact us through the National Relay Service
www.accan.org.au | info@accan.org.au | twitter: @ACCAN_AU

About ACCAN

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards communications services that are trusted, inclusive and available for all.

Consumers need ACCAN to promote better consumer protection outcomes ensuring speedy responses to complaints and issues. ACCAN aims to empower consumers so that they are well informed and can make good choices about products and services. As a peak body, ACCAN will represent the views of its broad and diverse membership base to policy makers, government and industry to get better outcomes for all communications consumers.

Contact

PO Box A1158,
Sydney South NSW, 1235
Email: info@accan.org.au
Phone: (02) 9288 4000
Contact us through the National Relay Service

Contents

1. Introduction 4
2. Responses to the discussion paper 5
   2.1. Effectiveness of the draft Determination 5
      2.1.1. Customer service and response times 5
      2.1.2. Flexibility and appropriateness of customer ID verification 6
      2.1.3. Consumers experiencing vulnerability 7
   2.2. High-risk customer interactions 8
   2.3. Multi-factor identity verification processes 9
   2.4. Identity verification requirements for customers in vulnerable circumstances 9
   2.5. Implementation 9
3. Final comments 10

1. Introduction

ACCAN appreciates the opportunity to provide feedback on the Telecommunications Service Provider (Customer Identity Verification) Determination.

It is evident from our consultations with our organisational members and the experiences of other consumer organisations and consumers across Australia, that scams and fraud against consumers is at an all-time high. Many telecommunications consumers have been placed at significant risk as a result of fraudulent activity conducted, without their knowledge or approval, on accounts they hold with telecommunications and other service providers. As the ACMA's discussion paper acknowledges, the prevalence of phone-based scams and identity theft is increasing at an alarming rate,[1] and it is essential that the telecommunications industry adopts additional safeguards to address current and future risks of scam and fraud-related consumer harm.[2]

ACCAN commends the ACMA for making this Determination and taking steps to protect consumers against fraudulent activity. Further, ACCAN submitted to the development of Industry Code C666:2021, Existing Customer Authentication,[3] and recognises the development of this Determination adds significant weight to the provisions of that Code and allows the ACMA, as the regulatory authority, a greater degree of latitude in terms of enforcement and compliance.

Whilst ACCAN broadly supports this Determination, concerns have been raised during our consultation with other consumer organisations about the need to ensure sufficient scope is inserted into the Determination to ensure that consumers experiencing vulnerability, and their agents, are able to conduct their business efficiently and without unnecessary bureaucracy. This is particularly important for people who, owing to disability, homelessness, cultural and linguistic barriers or financial difficulty, conduct their telecommunications business by use of a third-party such as a legal representative or financial counsellor. It is also important that this Determination takes into consideration the experiences of people for whom traditional sources of identification are difficult, such as people without drivers' licences, birth certificates or fixed addresses.

Additionally, whilst ACCAN appreciates the need to impose processes for appropriate means of determining the authenticity of requests, this may leave consumers experiencing vulnerability worse off, particularly as many telecommunications providers are reducing their human interactions with their customers and increasing the provision of online customer service. ACCAN is particularly concerned about the impact of using Artificial Intelligence and other digital means of verifying consumers' identity. It is vital that we address the need for timely and quality customer service and ensure that ID verification is flexible and appropriate to the means available to consumers experiencing vulnerability.

These concerns, and answers to the questions posed in the discussion paper, are detailed below.

---

[1] ACCC 2021, *Losses reported to Scamwatch exceed $211 million, phone scams exploding*, https://www.scamwatch.gov.au/news-alerts/losses-reported-to-scamwatch-exceed-211-million-phone-scams-exploding

[2] TIO 2021, *Systemic Investigation Report November 2021: Defending phone and internet accounts from fraudsters*, https://www.tio.com.au/sites/default/files/2021-11/Defending%20phone%20and%20internet%20accounts%20from%20fraudsters_fa_HiRes%20CLEAN.pdf

[3] https://accan.org.au/accans-work/submissions/1919-communications-alliance-industry-code-existing-customer-authentication

2. Responses to the discussion paper

2.1. Effectiveness of the draft Determination

ACCAN supports the draft Determination in principle and believes that applying multi-factor authentication to high-risk customer interactions will offer many consumers significant protection from fraudulent activity. The TIO's recent systemic issues investigation into telecommunications fraud found that fraudsters exploit weak ID verification processes of Retail Service Providers (RSPs), and at times, ID verification processes are not applied consistently by RSP staff.[4] This Determination should deliver a high and consistent threshold for customer ID verification.

ACCAN acknowledges the complexity of striking the right balance between preventing fraud through improved security and verification while ensuring that consumers are not unreasonably excluded from accessing or making changes to their accounts. People experiencing vulnerability and those with limited digital ability are disproportionately represented as fraud victims; unfortunately, people from these same cohorts are more likely to experience challenges verifying themselves to an RSP through rigid and automated ID authentication processes.[5]

ACCAN's key recommendation to the ACMA is that the draft Determination requires RSPs to ensure that:

- multi-factor authentication methods are, where necessary, appropriately flexible to meet the circumstances of the individual consumer.
- customer service related to ID verification issues and suspected scam or fraudulent activity is timely and of acceptable quality.

To this end, the draft Determination should address the following concerns that ACCAN has identified through consultation with members.

2.1.1. Customer service and response times

ACCAN's view is that no regulatory exercise can directly prevent every current and future risk of fraudulent activity; nor can a regulatory exercise prescribe an appropriate response to every circumstance in which a consumer has difficulty verifying their identity. Instead, RSPs must invest in quality and timely customer service – through resourcing, training, monitoring and reporting – so that they are equipped to respond appropriately to any circumstance.

Telecommunications consumer protection rules do not currently include benchmarks or requirements for RSPs to offer quality and readily available customer service.[6] Regrettably, there is evidence that

[4] TIO 2021, *Defending phone and internet accounts from fraudsters*, https://www.tio.com.au/sites/default/files/2021-11/Defending%20phone%20and%20internet%20accounts%20from%20fraudsters_fa_HiRes%20CLEAN.pdf

[5] ACCC 2021, Culturally and linguistically diverse community lose $22 million to scams in 2020, reports from Indigenous Australians up by 25 per cent, https://www.accc.gov.au/media-release/culturally-and-linguistically-diverse-community-lose-22-million-to-scams-in-2020-reports-from-indigenous-australians-up-by-25-per-cent

[6] ACCAN 2020, *ACCAN response to Consumer Safeguards Review Part C / Choice and Fairness*, https://accan.org.au/files/Submissions/2020/ACCAN%20Submission%20to%20Consumer%20Safeguards%20Review%20Part%20C%20V.1.1.pdf, p. 14

fraudsters exploit RSPs' poor customer service processes. The TIO has found that some RSPs do not act quickly when notified of an account security breach, and do not always implement customer ID authentication mechanisms consistently.[7] ACCAN receives regular feedback from members and consumers about cases where a customer has been prevented from accessing their accounts because they do not have access to certain account or personal information to verify their identity, and the RSP is unwilling to be flexible or use alternative ID verification methods. Resolving issues via RSPs' customer service can be extremely time consuming for consumers, as it takes an average of 2.3 separate contacts and 28 minutes to resolve a telco issue.[8] This is a relevant concern for ACCAN given that a delayed response from an RSP can make the impact of a security breach even worse.[9]

ACCAN is concerned that the draft Determination does little to ensure consumers have access to acceptable customer service in relation to ID verification or suspected fraud issues, regardless of who their RSP is.

In order to address this gap, and to ensure consumers are supported to access their accounts and take steps to prevent fraud if it is suspected, the draft Determination should:

- Direct providers of scale (for example, those with over 1,000 residential and small business customers) to establish a dedicated, well-resourced customer service channel specifically for account security and ID verification issues.
- Require providers to inform customers of their ID verification processes prior to high-risk interactions being undertaken.
- Amend the provision in Section (3)(a)(ii)[10] of the draft Determination to more explicitly require providers to notify the customer of the nature of suspected unauthorised access or fraud. Timeframes for notifying customers in Sections (3)(a)(ii)-(iii) should be specified.

2.1.2. Flexibility and appropriateness of customer ID verification

ACCAN has concerns about the way in which customer ID verification methods may be applied to people who are not able to verify themselves through the RSP's chosen verification methods. There are a number of reasons why conventional customer ID verification methods are not appropriate or accessible to consumers, for example:

- A regional, rural or remote consumer may not have access to mobile coverage for SMS-based multi-factor authentication, and may be unable to attend an RSP store to verify their identity.
- A recently-arrived migrant may not have current Australian Category A or B identity documents, and the RSP may choose not to recognise documentation from another country.
- A migrant may not feel safe providing identification information online, owing to privacy concerns or fears that the collection or use of personal information may affect their migration or visa status.

[7] TIO 2021, op. cit.

[8] ACCAN 2020, *Still Waiting … the cost of customer service*, https://accan.org.au/media-centre/media-releases/hot-issues/1825-still-waiting-the-cost-of-customer-service

[9] TIO 2021, op. cit.

[10] This section says that if a customer didn't authorise the high-risk account activity, they need to reverse the action, inform the customer about it, and notify the customer of what they can do to protect their identity.

- A person who is homeless or transient may not recall the address listed on their account.
- A person who has been affected by a natural disaster, for example a bushfire, may not have access to any documentation, and may not be in a position to recall their account details.
- A person may not have access to a smartphone to verify themselves using an in-app feature, or may not have a level of digital ability that allows them to do so.

Not all of these consumers may identify as being vulnerable, yet it is essential that RSP identity verification processes are appropriate and flexible to these circumstances and more.

The draft Determination does not explicitly prevent RSPs from insisting on certain ID verification methods. It should be explicitly articulated that, if a customer provides a reasonable explanation for why they cannot verify themselves through the RSP's chosen verification method, the RSP must work with the consumer to identify an appropriate alternative verification method. This could include:

- Matching customer ID documents (for example, a Drivers Licence) with a current photo of the customer holding those ID documents.
- Asking the customer to recall recent account activity, for example, the last recharge amount or the approximate time and length of recent phone calls made.
- Asking the customer to list other services and payments on the account, for example, Foxtel or sports subscriptions, device repayments, or third-party charges.

This flexibility should be granted to consumers regardless of whether they are identified or self-identify as experiencing vulnerability. Furthermore, safeguards should be put in place to ensure the alternative verification methods are working for consumers.

2.1.3. Consumers experiencing vulnerability

Section (11) of the draft Determination establishes practices for when an RSP has 'reasonable grounds' to believe that the requesting person is a customer in vulnerable circumstances. ACCAN's view is that current consumer safeguards, and many RSPs' practices, do not support the effective and proactive identification of telco consumers experiencing vulnerability adequately across the board.[11] In the absence of robust minimum standards regarding the identification and treatment of consumers experiencing vulnerability, the draft Determination should point to relevant guidance on this issue, for example:

- The anticipated ACMA Vulnerability Statement of Expectations.
- The ACCC Don't Take Advantage of Disadvantage Guideline.
- The ACCC/ASIC *Debt Collection Guideline for Collectors & Creditors*, that RSPs are required to adhere to under the Telecommunications Consumer Protections (**TCP**) Code.

Authorised Representatives and Advocates

ACCAN has concerns at how RSPs may adopt the draft Determination with respect to the activities of Authorised Representatives and Advocates (**consumer advocates**) given that many 'high-risk'

[11] ACCAN 2021, *ACMA Customer Vulnerability Statement of Expectations*, https://accan.org.au/accans-work/submissions/1920-acma-customer-vulnerability-statement-of-expectations

transactions are likely to be undertaken by consumer advocates, for example moving a service from post-paid to pre-paid, or cancelling services. ACCAN has undertaken extensive consultation with members regarding consumer advocates' experiences dealing with telcos, and our view is that current arrangements allow RSPs scope to impose significant administrative barriers on consumer advocates making changes to their clients' accounts. Additionally, there is evidence that RSPs do not always keep documentation regarding the appointment of a consumer advocate on hand. Further detail can be found in our submission on Industry Guidance Note 017: Authorised Representatives and Advocates.[12]

Ultimately, consumers bear the negative consequences of the administrative barriers imposed on Authorised Representatives and Advocates. There is little to no evidence to substantiate that fraudsters impersonate consumer advocates to gain access to consumers' accounts. In the absence of fair and consistent administrative processes regarding RSPs' dealings with consumer advocates, ACCAN's view is that the draft Determination should include a separate section which establishes that:

- A consumer has a right to appoint an Authorised Representative or Advocate, as specified in the TCP Code.[13]
- An Authorised Representative or Advocate who has provided evidence of legitimate authorisation (for example, an authority form on an official professional letterhead from a legitimate source, like an organisational email address) should not be barred from making changes to a customer's account due to multi-factor authentication issues.

Consumers fleeing Domestic and Family Violence

ACCAN is concerned that the draft Determination, particularly provisions related to informing the customer that high-risk activities have been initiated on their account, may place domestic and family violence (DFV) victim-survivors at risk, as their abusers may still be the primary account holder. RSPs are not required to have a DFV Response Policy, and the review of Communications Alliance's G660:2018 Assisting Customers Experiencing Domestic and Family Violence Guideline has stalled. This means that consumers fleeing DFV cannot be confident that they will receive fair and appropriate treatment by their telco in all circumstances.

Given the risks and likelihood of harm experienced by consumers fleeing DFV, and the absence of robust consumer safeguards protecting DFV victim-survivors, ACCAN strongly encourages the ACMA to undertake targeted consultation with DFV experts to understand the possible impact of the draft Determination on victim-survivors. It may be appropriate that the draft Determination sets out a separate communications process for consumers who self-identify as experiencing DFV.

2.2. High-risk customer interactions

ACCAN has consulted widely on this issue and is confident that the activities detailed in the Determination and discussion paper accurately represent activities which should be considered high-risk. It is important that sufficient consideration be given to ways in which the range of high-risk activities may change in the future, as well as to consider specific requirements for individual

[12] ACCAN 2019, *Feedback on Draft Authorised Representatives and Advocates Industry Guidance Note (IGN 017)*, https://accan.org.au/files/Submissions/CA%20IGN%20017_Authorised%20Representatives%20and%20Advocates%20feedback_FINAL.pdf

[13] Available: https://www.commsalliance.com.au/Documents/all/codes/c628

consumers. It is important that RSPs inform consumers about exactly which activities will be considered high risk and detail the extra steps consumers will have to undertake to ensure appropriate identity verification. Consistent with our comments above, service provider staff must have appropriate training to be able to identify consumers who may be experiencing vulnerability and ensure appropriate flexibility is given to properly allow them to conduct necessary activities.

2.3. Multi-factor identity verification processes

ACCAN is confident that a response period of 24 hours should be sufficient in most cases but it is important that the draft Determination considers the needs of individual consumers. RSPs must be required to discuss the need for this time period with their customers and flexibility should be afforded on a case-by-case basis to allow experiencing vulnerability or consumers who have specific needs, to provide the necessary authentication documents or to undertake alternate means of proof of identity. Customer Service staff should explain to the consumer that should they be unable to supply the appropriate authentication method within the discussed time, the request will lapse and the customer will have to make a new request. Preferably, the requirement for additional authentication documentation or methods should be discussed with the customer prior to the submission of any request for activity considered high risk. This discussion must occur in a culturally appropriate and accessible manner and ensure that information and advice provided by RSPs is easy for consumers to understand.

2.4. Identity verification requirements for customers in vulnerable circumstances

Please refer to ACCAN's response to Question 1 (above) for considerations related to consumers in vulnerable circumstances.

2.5. Implementation

Whilst ACCAN appreciates the need to move quickly in developing and implementing the Determination, it is vital that due consideration be given to the needs of consumers experiencing vulnerability and that the need to protect telecommunications consumers against scammers does not overshadow the need to ensure consumers can conduct their business safely and efficiently. It is important to consult with consumers and consumer organisations at each step along the process to ensure appropriate protections are put in place to protect their needs and to ensure that compliance with the Determination does not represent an undue burden on consumers.

Whilst an implementation date of 5 April 2022 is conceivable it is important that the development of measures designed to protect consumers with particular needs is not overlooked. In addition, given the quick development and implementation of the Determination, it will be important to review the Determination in the future to ensure it has not resulted in negative, unintended consequences for consumers, particularly consumers experiencing vulnerability.

3. Final comments

Whilst evidence clearly demonstrates the need for tighter regulation, it is important to allow flexibility both in the forms and methods of identity verification and the time allowed for consumers to prove their identity. More important though, is that RSP customer service staff understand all of the avenues consumers have available to them to prove their identities and to protect themselves against fraudulent activity. RSPs need to be aware of the ways in which scammers might try to gain control of a customer's account and be vigilant to protect customers against loss of vital services or negative financial and reputational implications from inappropriate use of their telco accounts.

ACCAN is available should any further clarification of our positions be required.