COMMUNICATIONS ALLIANCE LTD

# INDUSTRY CODE

# DR C666:2021

# EXISTING CUSTOMER AUTHENTICATION

DRAFT FOR PUBLIC COMMENT

Issued: 20th August 2021

Public comment close: 20th September 2021

**DR C666:2021 Existing Customer Authentication Industry Code**

**Communications Alliance Ltd was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.**

**Disclaimers**

1) Notwithstanding anything contained in this Industry Code:

   a) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct or indirect loss, damage, claim, or liability any person may incur as a result of any:

      i) reliance on or compliance with this Industry Code;

      ii) inaccuracy or inappropriateness of this Industry Code; or

      iii) inconsistency of this Industry Code with any law; and

   b) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Industry Code.

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

**Copyright**

# INTRODUCTORY STATEMENT

The Operations Reference Panel was tasked with reviewing Customer authentication principles to create an Industry Code designed to supplement other Industry regulation that seeks to provide a wholistic approach to authentication of a person seeking to take action that affects the use of a telecommunication service.

This Code together with the associated Industry Guideline **Existing *Customer Authentication*** Industry Guideline (G668:2021) is designed to provide:

- a common set of principles for ensuring that CSP's have strong protections in place to authenticate that a request to undertake an activity associated with supply of a carriage service has sufficient rigour to limit fraudulent activity that may affect the Customer;

- that a request to undertake an activity is being made by the customer or their Authorised Representative and has adequate authentication that is consistent with the level of risk that arises from the requested action;

- limits to the opportunity for fraudulent activity, in particular any action that could result in the customer losing access to their telecommunications service (e.g. via SIM swap or service transfer).

The Code seeks to provides a framework for an approach to customer authentication that includes:

(i) a focus on desired outcomes (rather than process);

(ii) allows flexibility in how and when telecommunications providers use additional authentication measures to enable customers to use and make changes associated with use of their carriage service without undue delay';

(iii) provides easy to use flexible approaches to authentication that do not cause difficulties for those customers who are vulnerable or have special needs; and

(iv) requires CSPs to provide information to their Customers so that they are aware of the authentication solutions that will apply to particular actions associated with the supply of the carriage service in a time and a way that makes sense to each provider authentication arrangements and their Customers.

The intended result is for targeted approaches to existing customer authentication to limit the opportunity for fraud.

Alexander R. Osborne
Chair
***Operations Reference Panel***

AUGUST 2021

# TABLE OF CONTENTS

# 1 GENERAL

## 1.1 Introduction

1.1.1 Section 112 of the *Telecommunications Act 1997* (the Act) sets out the intention of the Commonwealth Parliament that bodies and associations representing sections of the telecommunications industry develop industry codes relating to the telecommunications activities of participants in those sections of the industry.

1.1.2 The development of the Code has been facilitated by Communications Alliance through a Working Committee comprised of representatives from the telecommunications industry.

1.1.3 The Code should be read in the context of other relevant codes, guidelines and documents.

1.1.4 The Code should be read in conjunction with related legislation, including:

(a) the Act;

(b) the *Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth)*;

(c) the *Competition and Consumer Act 2010 (Cth);*

(d) the *Privacy Act 1988 (Cth); and*

(e) the *Telecommunications (Mobile Number Pre-Porting Additional Verification) Industry Standard 2020*.

1.1.5 If there is a conflict between the requirements of the Code and any requirements imposed on a Supplier by statute, the Supplier will not be in breach of the Code by complying with the requirements of the statute. Compliance with this Code does not guarantee compliance with any legislation. The Code is not a substitute for legal advice.

1.1.6 Statements in boxed text are a guide to interpretation only and not binding as Code rules.

## 1.2 Registration by the ACMA

The Code is to be submitted to the Australian Communications and Media Authority for registration under to section 117 of the Act.

## 1.3 Scope

1.3.1 The Code applies to the Carriage Service Providers section of the telecommunications industry under section 110 of the Act.

1.3.2 It deals with the following telecommunications activities as defined in section 109 of the Act:

(a) carrying on business as a Carrier; or

(b) carrying on business activities as a Carriage Service Provider; or

(c) supplying Goods or Service(s) for use in connection with the supply of a Listed Carriage Service.

1.3.3 The Code applies to residential and small business customers and regulates matters relating to the authentication of a Requesting Person where the Requesting Person is seeking to conduct a transaction on / or to gain access to information of an account or Telecommunications Service.

1.3.4 The Code does not apply to matters covered by codes or standards registered or determined under the *Broadcasting Services Act 1992* (Cth) as required by section 116 of that Act.

1.3.5 The Code does not apply to procedures relating to the onboarding of new Customers.

## 1.4 Objectives

1.4.1 The objectives of the Code are:

(a) to set out procedures for appropriate Customer Authentication measures for existing Customers;

(b) to reduce harm to Customers from unauthorised actions performed on their accounts; and

(c) the protection of Customer data from unauthorised access.

## 1.5 Code review

1.5.1 The Code will be reviewed after 2 years of the Code being registered by ACMA and every 5 years subsequently, or earlier in the event of significant developments that affect the Code or a chapter within the Code.

# 2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

## 2.1 Acronyms

For the purposes of the Code:

**ACMA**

means the Australian Communications and Media Authority.

**CSP**

means Carriage Service Provider.

**MMS**

means Multimedia Message Service.

**OTP**

means One Time Passcode.

**SIM**

means Subscriber Identity Module.

**SMS**

means Short Message Service.

## 2.2 Definitions

For the purposes of the Code:

***Act***

means the *Telecommunications Act 1997 (Cth)*.

***Authorised Representative***

has the meaning given by the Telecommunications Consumer Protections Code (C628:2019).

***Biometric data***

has the meaning given by section 6 of the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020.

***Carriage Service Provider***

has the meaning given by section 87 of the Act.

***Carrier***

has the meaning given by section 7 of the Act.

***Consumer***

means:

(a) an individual who acquires or may acquire a Telecommunications Product for the primary purpose of personal or domestic use and not for resale; or

(b) a business or non-profit organisation which acquires or may acquire one or more Telecommunications Products which are not for resale and, at the time it enters into the Customer Contract, it:

i. does not have a genuine and reasonable opportunity to negotiate the terms of the Customer Contract; and

ii. has or will have an annual spend with the Supplier which is, or is estimated on reasonable grounds by the Supplier to be, no greater than $40,000, or, in the 5 months following Code commencement, an annual spend of $20,000.

A reference to a Consumer includes a reference to the Consumer's Authorised Representative.

A reference to a Consumer includes a reference to a Customer.

**Customer**

means a Consumer who has entered into a Customer Contract with a Supplier.

A reference to a Customer includes a reference to the Customer's Authorised Representative.

**Customer Authentication**

means the process of validating a person is the Customer by way of verifying and comparing proof of identity credentials with that information held or acknowledged by a C/CSP.

**Government Online Verification Service**

has the meaning given by section 6 of the *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020.*

***Multi factor authentication***

means an authentication process that uses 2 or more authentication factors to verify the identity of a Requesting Person.

***One Time Passcode***

means a unique time limited code sent to a previously agreed Public Number or email address for a Telecommunications Service, to help authenticate the Customer through their access to the contact details associated to that Telecommunications Service.

***Public Number***

means those numbers as defined in section 16 of the *Telecommunications Numbering Plan 2015*. taken be used to supply a Carriage Service to a CSP or a Customer as in section 44 of the Act.

***Requesting Person***

*means the person contacting the CSP to conduct a transaction on / or gain access to information of a Telecommunications Service*.

***Supplier***

means a Carriage Service Provider.

**Telecommunications Service**

has the meaning given by the Telecommunications Consumer Protections Code (C628:2019).

## 2.3 Interpretations

In the Code, unless the contrary appears:

(a) headings are for convenience only and do not affect interpretation;

(b) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(c) words in the singular includes the plural and vice versa;

(d) words importing persons include a body whether corporate, politic or otherwise;

(e) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(f) mentioning anything after include, includes or including does not limit what else might be included;

(g) words and expressions which are not defined have the meanings given to them in the Act; and

(h) a reference to a person includes a reference to the person's executors, administrators, successors, agents, assignees and novatees.

# 3 GENERAL RULES

The general rules for Customer Authentication.

## 3.1 Customer Authentication Measures

3.1.1 A CSP must have authentication measures or security practices in place to verify the Requesting Person's identity, commensurate with the risk of the transaction requested to be undertaken, and the path it is being conducted through.

3.1.2 A CSP must designate transaction types based on the Customer impact of the associated transaction.

3.1.3 A CSP must ensure that the authentication measures or security practices are consistent with the value and potential risk to the Customer of the transaction.

3.1.4 A CSP must designate certain transaction types as high-risk transactions which require a higher level of Customer Authentication.

3.1.5 Where a CSP cannot authenticate the Customer through an appropriate form of verification or appropriate security measure, the transaction requested should not be undertaken until the CSP is reasonably satisfied the Requesting Person is the Customer.

## 3.2 Risk Based Activities

3.2.1 Customer service approaches must consider what information may be publicly accessible and how that may be used by those with criminal intent to access a customer's service.

3.2.2 Customer facing customer service solutions must ensure appropriate levels of Customer Authentication.

| NOTE: These solutions should use visual identity documents e.g., a Government Document. |
|---|

3.2.3 Solutions must rely on data that is only available to the Customer. Where possible, these should be a combination of at least one knowledge authenticator and followed by at least one Biometric Data or possession authenticator.

<u>Inbound Customer Authentication – Customer contacting CSP</u>

3.2.4 For inbound communications, CSPs must only confirm and never disclose Customer personal information without proper Customer Authentication.

3.2.5 CSPs must ensure that all high-risk transactions are secured using Multi Factor Authentication or other appropriate security measures.

Outbound Customer Communications – CSP contacting Customer.

3.2.6 For outbound communications which requires a CSP to Authenticate a Customer, a CSP must consider whether alternative Customer Authentication processes can be used instead of asking Customers for their security or sensitive information.

> NOTE: If this is not possible, the CSP should provide Customers with an easy way to contact them if a Customer would like to check the communication is authentic before they provide any personal information.

3.2.7 A CSP must remove high-risk transactions from outbound communications unless Multi Factor Authentication is performed.

> NOTE: If available, CSPs should promote Customer self-service for processing of high-risk transactions.

**High Risk Transactions**

3.2.8 CSPs must ensure all high-risk transactions are secured via Multi Factor authentication.

> NOTE: If available, CSPs should promote Customer self-service for processing of high-risk transactions or the use of a 2-way communication system that includes text-based information for high-risk transactions to allow the account holder to review and approve.

**Other Transactions**

3.2.9 CSPs must ensure all other transactions are secured via at least one factor of authentication.

> NOTE: Where multi factor authentication has not been used to access the method of enacting the high-risk transaction, at that time, a One Time Passcode or account PIN should not be used as a single identification factor.

## 3.3 Multi Factor Authentication

3.3.1 A first authenticator must be a knowledge authenticator that is not publicly available and only the Customer should know.

3.3.2 Further authenticators must be a Biometric Data method or a possession authenticator that validates that the Customer is either physically in possession of the service or has access to their personal email box or app which also requires a password, or other form of authentication.

3.3.3 CSP's must not use two forms of authentication from the same category, unless the individual Customer could not reasonably be expected to be able to provide a response to possession authenticators.

## 3.4 Customer information requirements

3.4.1 A CSP must publish information on its website advising customers that:

(a) to protect Customers from unauthorised transactions, additional identity verification processes will be used; and

(b) in the event a customer suspects that their service has been fraudulently accessed they should immediately report the activity to:

i. their CSP;

ii. the Australian Federal Police or the relevant State or Territory Police; and

iii. government services that support customers whose service may have been subject to fraud.

# 4 REFERENCES

| Publication | Title |
|---|---|
| **Industry Codes** | |
| C628:2019 | Telecommunications Consumer Protections Code |
| | |
| **Industry Guidelines** | |
| G668:2021 | Existing Customer Authentication |
| **Legislation** | |
| *Privacy Act 1988* | |
| *Telecommunications Act 1997* | |
| *Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth)* | |
| *Competition and Consumer Act 2010 (Cth);* | |
| *Telecommunications (Mobile Number Pre-Porting Additional Verification) Industry Standard 2020* | |

# PARTICIPANTS

The Working Committee that developed the Code consisted of the following organisations and their representatives:

| Organisation | Membership | Representative |
|---|---|---|
| AMTA | Non-voting | Lisa Brown |
| Amaysim | Voting | Chad Heininger |
| MNF Group | Voting | Geoff Brann |
| MNF Group | Non-voting | Christopher Hooker |
| Optus | Voting | Warren Hudson |
| Optus | Non-voting | Nerelie Green |
| Telstra | Voting | David Fabbian |
| Telstra | Non-voting | James Wu |
| TPG Telecom | Voting | Annie Leahy |
| TPG Telecom | Non-voting | Alexander R. Osborne |
| Vocus | Voting | John Sexton |

This Working Committee was chaired by Alexander R Osborne. Craig Purdon of Communications Alliance provided project management support.

Communications Alliance was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507