COMMUNICATIONS ALLIANCE LTD

INDUSTRY CODE

C666:2021

EXISTING CUSTOMER AUTHENTICATION

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

EXPLANATORY STATEMENT

This is the Explanatory Statement for the C666:2021 **Existing Customer Authentication** Industry Code (the Code).

This Explanatory Statement outlines the purpose of the Code and the factors that have been taken into account in its development.

The objective of the Code is to set out procedures for appropriate Customer Authentication measures for existing Customers in order to assist in achieving the outcomes of:

(a) reducing the risk of harm to Customers from unauthorised actions performed on their accounts; and

(b) the protection of Customer information from unauthorised access.

Why a Code is required

The Code provides a positive framework for an industry approach to Customer Authentication with the intended result of reducing the opportunity for and impacts from fraud.

With those that attempt to commit fraud employing various and sophisticated ways of attempting to defraud unsuspecting victims, industry is acutely aware of the need to be nimble, innovative and flexible in their approaches to protecting their Customers and maintain trust in the security of their Telecommunications Service, while at the same time not affecting the ability of genuine customers, especially those who are vulnerable, disadvantaged or in an emergency situation from being able to conduct activity with their CSP.

Background

Fraud is an ongoing risk to both consumers, the telecommunications industry and society.

Every day there are those who seek to defraud consumers and the level of sophistication and agility now seen by those seeking to undertake fraudulent activity is one of the key issues faced by industry.

The industry has applied a range of solutions to limit fraudulent activity over many years, however many consumers are still affected by fraud and even well informed and sophisticated consumers are not immune to its effects.

Protecting Customers from fraudulent activity has been an ongoing process since 2009, it is not something new for Industry. In 2009 The Industry Code C570 Mobile Number Portability was modified to enable financial institutions to access data to investigate and limit fraud by improving access to information. More recently in 2018, Mobile Carrier and Carriage Service Providers (CSPs) first began drafting guidance for industry regarding measures to strengthen mobile number portability processes.

In March 2019, the ACMA released a consultation paper seeking comment on Combating Scams and Technological Solutions, and the focus moved on to addressing scam calls. The then Minister for Communications and the Arts and the ACMA established the cross-agency Scam Technology Project (the Project) with the ACCC and the Australian Cyber Security Centre (ACSC), to explore ways to reduce scam activity.

April 2020 saw the commencement of the *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020,* which was developed by the ACMA under instruction from the Hon Paul Fletcher Minister for Communications, Urban Infrastructure, Cities and the Arts. The Standard being a construct of the work previously begun by Industry in 2018.

December 2020 saw the registration by the ACMA of the Reducing Scam Calls Industry Code C661:2020.

Current Regulatory Arrangements

This Code fits within an existing regulatory scheme that comprises:

(a) the *Telecommunications Act 1997*;

(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.

How the Objectives are achieved

This Code is made under Part 6 of the *Telecommunications Act* and upon their satisfaction that certain statutory criteria has been met, is registered by the ACMA. Upon registration (this process applies to each revision of the Code), the Code becomes mandatory on all Carriage Service Providers (CSP).

Following registration, if there is a contravention of this Code, the ACMA may warn a CSP about the contravention or direct them to comply with the Code. Failing to comply with a direction may render the CSP liable to significant financial penalties.

Anticipated Benefits to Consumers and the Public

The Code seeks to provide a consistent and flexible approach to Existing Customer Authentication to minimise, wherever possible, fraudulent activities being undertaken on a customer's telecommunications service without the customers knowledge, and to limit the financial and emotional impacts from such fraudulent activity.

Anticipated Benefits to Industry

The revised Code provides an obligation to improve customer authentication, identify potential risks and address them. The Code specifically does not identify what types of transaction need additional authentication and does not identify how a CSP will carry out this task, as to do so would provide information that would allow those that commit fraud to circumvent them. This Code will lead to improved authentication of processes across a number of transactions which CSP's undertake daily with their customers. The Code also seeks to maintain trust from customers that their CSP is protecting their telecommunications service interactions and data from unauthorised access.

Anticipated Costs to Industry

Training programs for industry members to raise awareness of the changes and impacts of the Code and ensure compliance, will always be an ongoing cost. System improvements will require IT development, and there may be associated costs with the development of customer service tools to provide additional contact options for customers.

Anticipated Costs to Consumers and the Public

The costs to consumers and the public should be minimal as there is no need for consumers to implement any changes apart from educating themselves on the additional security measures which may be required when interacting with their CSP.

INTRODUCTORY STATEMENT

The Operations Reference Panel was tasked with reviewing Customer Authentication principles to create an Industry Code designed to limit fraudulent activity by supplementing other measures that seek to provide a holistic approach to authentication of a Requesting Person that seeks to access customers information or to take action that affects the use of a Listed Carriage Service.

Limiting fraudulent activity and undertaking a requested action is a multi-layered activity. In some cases, the action of authenticating that a Requesting Person is the Customer may be sufficient to enable a CSP to proceed with the requested action where the Requesting Person is confirmed as the Customer, such as providing account information, replacing non-functional equipment provided as part of the service, such as a damaged modem. In other transactions a Customer may also have to authorise an activity, such as those involving an additional cost, by way of providing authorisation by way of a signature or electronic authorisation.

This Code together with the associated **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 Requesting Person is the Customer and therefore able to undertake an activity associated with supply of a Listed Carriage Service with 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 of harm 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 CSP's use additional authentication measures to enable Customers to use and make changes associated with use of their Listed Carriage Service without undue delay;

iii. provides easy to use flexible approaches to Customer Authentication as recognition that a one size fits all approach may limit the ability of Customers who are vulnerable, disadvantaged or those affected by emergency situations to perform a requested action; 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.

Where a Requesting Person has been appropriately authenticated as the Customer, based on the transaction being undertaken, the Code does not generally require further authentication for each transaction requested by the Customer, as part of the same contact session with the

CSP. The only exception is where an initial request for one or more transactions that are not High Risk is followed by a request for a High-Risk transaction. In this situation, the High-Risk Transaction must not proceed until any additional authentication required for the High-Risk Transaction has been completed.

The Code does not limit a CSP from choosing to apply additional authentication to each transaction.

The Code does not replace commercial arrangements or obligations associated with the requested action where the requested action requires a Customer authorisation such as by way of a signature or electronic authorisation, for such transactions associated with an ongoing financial obligation, for example, adding additional services to an account, agreeing a payment plan for new equipment, etc.

The intended result is for targeted approaches to existing Customer Authentication to limit the opportunity for fraud.

Alexander R. Osborne
Chair
Operations Reference Panel

October 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 including:

(a) the Existing Customer Authentication Guideline (G668:2021); and

(b) the Telecommunications Consumer Protections Code (C628:2019).

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 carrying on business activities as a Carriage Service Provider, a telecommunications activity as defined in section 109 of the Act.

1.3.3 The Code applies to Carriage Service Providers in respect of their relationship with existing Customers, and regulates matters relating to the authentication of a Requesting Person where the Requesting Person is seeking to:

(a) conduct a transaction in relation to a Telecommunications Service; or

(b) 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.

NOTE: These procedures are covered by arrangements under the Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017 and the Telecommunications Consumer Protections Code (C628:2019).

1.3.6 The Code commencement date for Consumers is 5 April 2022.

1.3.7 The Code commencement date for Large Business Customers is 5 July 2022.

NOTE: The ACMA at its discretion may consider any extension to these implementation timeframes on a case-by-case basis.

1.4 Objectives

1.4.1 The objective of the Code is to set out procedures for appropriate Customer Authentication measures for existing Customers in order to assist in achieving the outcomes of:

(a) reducing the risk of harm to Customers from unauthorised actions performed on their accounts; and

(b) the protection of Customer information 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:

CSP

means Carriage Service Provider.

PIN

means Personal Identification Number

SIM

means Subscriber Identity Module.

2.2 Definitions

For the purposes of the Code:

Act

means the *Telecommunications Act 1997 (Cth)*.

Authorised Representative

means a person who has authority from a Customer to deal with a Supplier, including to discuss or make changes to the Customer's account without that Customer being present, on behalf of that Customer.

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.

Category A Document

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

Category B Document

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

Consumer

means:

a) a person who has an existing Telecommunications Service for the primary purpose of personal or domestic use and not for resale; or

b) a business, or non-profit organisation which has an existing Telecommunications Service which is not for resale, and, at the time it entered into the Customer Contract, it

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

   ii. had or would 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.

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

Customer

means a person who has entered into a Customer Contract with a Supplier and includes Consumers and Large Business Customers (as applicable).

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 CSP.

Customer Contract

means an arrangement or agreement between a Supplier and a Consumer or Large Business Customer for the supply of a Telecommunications Service to that Consumer or Large Business Customer.

NOTE: For the avoidance of doubt, unless stated otherwise, the standard form customer contract is a Customer Contract.

Government Online Verification Service

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

High-Risk Transactions

means any transaction that may result in one or more of the following outcomes:

(a) the Customer losing access to their Telecommunications Service;

(b) a change to any information held or acknowledged by the CSP as relating to the identity of the Customer; and

(c) a high value charge is applied, or will be applied to the Customer's account.

NOTE: High-Risk Transactions may include, but are not limited to:

- *SIM swap*
- *Viewing or changing unique internal identifiers, Customer name, DOB, email, password, payment or contact details;*
- *changing an authorisation access method (e.g. PIN, password, IMEI or IMSI);*
- *enabling call diversion;*
- *enabling call barring;*
- *purchases over a defined limit.*

Large Business Customer

means an entity who has an existing Telecommunications Service:

(a) for the primary purpose of a business, not-for-profit or government organisation; and

(b) which is not for resale; and

(c) which at the time it entered into the Customer Contract:

i. had a genuine and reasonable opportunity to negotiate the terms of the Customer Contract; and / or

ii. had or would have an annual spend with the CSP which is or is estimated on reasonable grounds by the provider to be greater than $40,000.

A reference to a Large Business Customer includes a reference to their Authorised Representative.

Listed Carriage Service

has the meaning given by section 16 of the Act.

Multi-Factor Authentication

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

Requesting Person

means the person contacting the CSP to;

(a) undertake a transaction in relation to a Telecommunications Service; or

(b) gain access to information relating to a Telecommunications Service.

Supplier

means a Carriage Service Provider.

Systems Integration Channel

means the use of APIs (Application Programming Interfaces) or a similar agreed electronic data exchange layer for the purposes of enabling machine-to-machine integration between a Large Business Customer system and a Carriage Service Provider system.

Telecommunications Service

means a Listed Carriage Service.

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 Customer Authentication measures or security practices in place to verify whether a Requesting Person is a Customer.

3.1.2 A CSP must designate High-Risk Transactions based on whether the transaction relates to a Consumer or Large Business Customer, and what will be the impact of the associated transaction and the potential risk of harm to the Customer of the transaction.

> *NOTE: High-Risk Transactions require a higher level of Customer Authentication. Different types of transactions may be considered High-Risk Transactions for Consumers and Large Business Customers.*

3.1.3 A CSP must ensure that the Customer Authentication measures, or security practices are commensurate with the value and potential risk of harm to the Customer of the transaction.

3.1.4 Where a CSP cannot authenticate that a Requesting Person is a Customer through Customer Authentication measures or appropriate security practice, the transaction requested should not be undertaken by the CSP until the CSP is reasonably satisfied the Requesting Person is the Customer.

3.2 Risk Based Activities

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

3.2.2 CSPs must ensure that customer facing service solutions implement appropriate levels of Customer Authentication, which may include electronic forms of authentication, or verifying the identity of the Requesting Person by viewing either;

- 1 Category A Document (identifying the Customer); or
- 2 Category B Documents, each of a different kind (identifying the Customer).

> NOTE: Refer to the *Telecommunications (Mobile Number Pre-Porting Additional Verification) Industry Standard 2020* for a list of examples.

3.2.3 Customer Authentication measures and security practices must rely on data that is only available to the Customer. Where possible, these should be, Multi-Factor Authentication which combines at least two of the following;

i. at least one knowledge factor:

ii. a possession factor;

iii. an inherent factor of Biometric Data.

Inbound Customer Authentication – Requesting Person contacting CSP

3.2.4 For inbound communications from a Requesting Person (e.g. in store, telephone, email, text, chat service etc.) relating to all transactions, a CSP;

(a) may only confirm the Requesting Person's personal information; and

(b) must never disclose Customer personal information unless the CSP has verified the identity of the Requesting Person and confirmed the Requesting Person is the Customer.

NOTE: Inbound communications for the reporting of faults are not considered High-Risk Transactions.

Outbound Customer Communications – CSP contacting Customer.

3.2.5 For outbound communications (e.g. telephone, email, text, chat service etc) related to High-Risk Transactions a CSP should:

(a) only contact Customers via a previously verified method; and

(b) avoid asking Customers for their security or personal information.

NOTE: Outbound communications such as marketing mail, outage notifications are not considered High-Risk Transactions.

3.2.6 For all outbound communications, a CSP must have at least one Customer Authentication process that can be used instead of verbally asking Customers for their security or personal information.

3.2.7 For all outbound communications a CSP;

(a) may only confirm the Customer's personal information; and

(b) must never disclose Customer personal 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.

3.2.8 A CSP must remove High-Risk Transactions from outbound communications with Customers unless Multi-Factor Authentication is performed.

NOTE: If available, CSPs should promote Customer self-service for processing of High-Risk Transactions.

High Risk Transactions

3.2.9 CSPs must ensure all High-Risk Transactions are secured via Multi-Factor Authentication or by a Systems Integration Channel.

3.2.10 A CSP must disclose to the Large Business Customer which High Risk Transactions are possible via a Systems Integration Channel.

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 Customer to review and approve the High-Risk Transaction.

Methods of self-service should be universally accessible and comply with the latest Web Content Accessibility Guidelines (WCAG) standards to ensure full accessibility for people with a disability. Self-service options should also consider Customers that may have other factors that limit their ability to use a self-service facility.

Visual authentication options should be available for Customers who cannot use online services, or who do not have the appropriate technology or skills to use a self-service method.

Other Transactions

3.2.11 CSPs must ensure all other non-High-Risk Transactions, (excluding those concerning disclosure of general information not related to Customer account information, which do not require any authentication) are secured via at least one factor of authentication.

3.3 Multi-Factor Authentication

3.3.1 Multi-Factor Authentication combines at least two of the following:

i. A knowledge authenticator that is not publicly available and only the Customer should know.

ii. A possession authenticator that validates that the Customer is either physically in possession of the service or has access to an email address or app which is connected to the service and which also requires a password, or other form of authentication (where practicable).

iii. An inherent authenticator such as a possession authenticator or Biometric Data that validates the Customer is who they claim to be.

3.3.2 CSP's must not use two forms of authentication from the same category, as per clause 3.3.1, unless the Customer or Requesting

Person could not reasonably be expected to be able to provide a response to possession or biometric authenticators.

3.4 Customer information requirements

3.4.1 A CSP must publish information on its website advising Customers how to protect themselves from unauthorised transactions and who to inform in case of their details being disclosed.

3.5 Training

3.5.1 A CSP must ensure relevant customer-facing staff are appropriately trained in the Customer Authentication measures and security practices it employs, including how to recognise activities which may have a potential to lead 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	
Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017	

PARTICIPANTS

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

Organisation	Membership	Representative
Amaysim	Voting	Chad Heininger
AMTA	Non-voting	Lisa Brown
MNF Group	Voting	Geoff Brann
Optus	Voting	Warren Hudson
Optus	Non-voting	Nerelie Green
Telstra	Voting	Brian Miller
Telstra	Non-voting	David Fabbian
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