

**COMMUNICATIONS  
ALLIANCE LTD**



INDUSTRY CODE

DR C661:2020

REDUCING SCAM CALLS

DRAFT FOR PUBLIC COMMENT

Issued: 24<sup>th</sup> March 2020

Public comment close: 8<sup>th</sup> May 2020

## **DR C661:2020 REDUCING SCAM CALLS Industry Code**

This Code is issued in draft form for public comment as DR C661:2020

**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**

© Communications Alliance Ltd 2020

This document is copyright and must not be used except as permitted below or under the Copyright Act 1968. You may reproduce and publish this document in whole or in part for your or your organisation's own personal or internal compliance, educational or non-commercial purposes. You must not alter or amend this document in any way. You must not reproduce or publish this document for commercial gain without the prior written consent of Communications Alliance. Organisations wishing to reproduce or publish this document for commercial gain (i.e. for distribution to subscribers to an information service) should apply to Communications Alliance by contacting the Communications Alliance Commercial Manager at [info@commsalliance.com.au](mailto:info@commsalliance.com.au).

## **INTRODUCTORY STATEMENT**

Scam Calls annoy and defraud Australian consumers. While vulnerable consumers are at the highest risk of being defrauded, even well informed and sophisticated consumers can fall victim. Even those not defrauded are victims to an extent, as their telecommunications service is used to persistently deliver Scam Calls or in some cases their number is used (spoofed) to make Scam Calls without their knowledge.

The level of sophistication and agility now seen with scammers and fraudsters is one of the key issues faced by industry. In addition to the work being undertaken by the regulators to combat scammers and fraudsters, industry is also developing a range of technical responses to reduce Scam Calls.

This Code sets out a process for identifying, tracing, blocking and otherwise disrupting Scam Calls. The process is built on improved information sharing between Carriers/Carriage Service Providers (C/CSPs) as well as improved information sharing between industry and regulators. The Code provides a framework for co-operation that industry believes will ultimately lead to the identification of scammers so enforcement action can be taken. Along the way, a number of disruptive measures will be introduced which industry expect will also reduce the number of Scam Calls reaching Australian consumers.

John Laughlin  
Chair

**WC92 Reducing Scam Calls Working Committee**

MARCH 2020

## TABLE OF CONTENTS

<b>1</b>	<b>GENERAL</b>	<b>2</b>
1.1	Introduction	2
1.2	Registration by the ACMA	2
1.3	Scope	3
1.4	Objectives	3
1.5	Code review	3
1.6	Powers of the Telecommunications Industry Ombudsman (TIO) to handle complaints under the Code	4
<b>2</b>	<b>ACRONYMS, DEFINITIONS AND INTERPRETATIONS</b>	<b>5</b>
2.1	Acronyms	5
2.2	Definitions	6
2.3	Interpretations	8
<b>3</b>	<b>CONSUMER INFORMATION</b>	<b>9</b>
3.1	Education about scam calls	9
<b>4</b>	<b>SCAM CALLS</b>	<b>10</b>
4.1	Characteristics of Scam Calls	10
4.2	Identifying Scam Calls	10
4.3	Improving CLI accuracy	11
4.4	Monitoring for Scam Calls	12
4.5	Tracing Scam Calls	12
4.6	Blocking Scam Calls	13
4.7	Blocking calls from International Operators	13
<b>5</b>	<b>C/CSP CONTACT LIST</b>	<b>14</b>
<b>6</b>	<b>REFERENCES</b>	<b>15</b>
	<b>APPENDIX</b>	<b>16</b>
<b>A</b>	<b>SAMPLE FOR INFORMATION SHARING REQUEST</b>	<b>16</b>
	<b>PARTICIPANTS</b>	<b>17</b>

# 1 GENERAL

## 1.1 Introduction

- 1.1.1 Section 112 of the *Telecommunications Act 1997 (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 and ACMA.
- 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)*;
  - (e) the *Spam Act 2003 (Cth)*; and
  - (f) the *Do Not Call Register Act 2006 (Cth)*.
- 1.1.5 If there is a conflict between the requirements of the Code and any requirements imposed on a C/CSP by statute, the C/CSP will not be in breach of the Code by complying with the requirements of the statute.
- 1.1.6 Compliance with this Code does not guarantee compliance with any legislation. The Code is not a substitute for legal advice.
- 1.1.7 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 (ACMA) for registration under section 117 of the Act. The ACMA may register a Code where it is satisfied that relevant considerations are met, including that the Code provides adequate community safeguards for the matters to be covered and that adequate consultation has been undertaken.

### 1.3 **Scope**

- 1.3.1 The Code applies to the Carriers and CSP section of the telecommunications industry under section 110 of the Act.
- 1.3.2 The Code 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 CSP; or
  - (c) supplying goods or service(s) for use in connection with the supply or enablement of a Listed Carriage Service.
- 1.3.3 The Code applies to Scam Calls that target customers and the obligations in sections 287, 289 & 313 (1) of the Act and section 474.17 of the *Criminal Code Act*.
- 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.

### 1.4 **Objectives**

- 1.4.1 The objectives of the Code are to:
  - (a) define Scam Calls in the context of the Code;
  - (b) establish processes by which C/CSPs will work with each other and the regulators to identify and handle Scam Calls;
  - (c) establish processes to share and communicate evidence of Scam Calls between C/CSPs and the regulators;
  - (d) establish processes for C/CSPs to exchange information in order to trace the origin of Scam Calls;
  - (e) establish a process for C/CSPs to block Scam Calls (from specific A-Party CLI(s) and
  - (f) establish a process to reinstate calls from blocked A-Party CLI(s).

### 1.5 **Code review**

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

1.6 **Powers of the Telecommunications Industry Ombudsman (TIO) to handle complaints under the Code**

- 1.6.1 The Code does not confer powers or functions on the TIO under section 114 of the Act.

## 2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

### 2.1 Acronyms

For the purposes of the Code:

**ACCC**

means the Australian Competition and Consumer Commission.

**ACMA**

means the Australian Communications and Media Authority.

**CA**

means Communications Alliance.

**CDR**

means Call Data Record.

**CND**

means Calling Number Display.

**CLI**

means Calling Line Identification.

**CSP**

means Carriage Service Provider.

**C/CSP**

means Carrier or Carriage Service Provider.

**PABX**

means Private Automatic Branch Exchange.

**PIN**

means Personal Identification Number.

**SMS**

means Short Message Service.

**UTC**

means Coordinated Universal Time.

**XPOI**

means across the point of interconnection between C/CSPs.

## 2.2 Definitions

For the purposes of the Code:

### **Act**

means the *Telecommunications Act 1997 (Cth)*.

### **A-Party**

means the individual or entity initiating the communication.

### **B-Party**

means the individual or entity receiving the communication.

### **Business Day**

means any day from Monday to Friday (inclusive) excluding any day that is gazetted as a public holiday, for the relevant jurisdiction, in a Commonwealth, State or Territory gazette.

### **Calling Line Identification**

means the data generated by a Telecommunications Network which relates to the Public Number of the A-Party.

### **Calling Number Display**

means the displayed or presented Public Number and/or name of the A-Party (based on CLI).

### **Carriage Service**

has the meaning given by section 7 of the Act.

*NOTE: For the purposes of this Code, a Carriage Service means:  
voice telephony that is supplied to, or used by, an A-Party or B-Party within Australia.*

### **Carriage Service Provider**

has the meaning given by section 87 of the Act.

### **Carrier**

has the meaning given by section 7 of the Act.

### **CLI Spoofing**

means the unauthorised use of a Public Number issued to a customer, where the A-Party is not the customer to whom that Public Number was issued, and where the A-Party has injected a false CLI in an attempt to deliberately mask or mislead the B-Party about the identity of the originating caller.

***International Operator***

means an entity based outside of Australia which connects with and passes call traffic to an Australian Transit C/CSP.

***Listed Carriage Service***

has the meaning given by section 16 of the Act.

***Notifying C/CSP***

means a C/CSP who believes it has identified Scam Calls being delivered onto its network and provides details of the Scam Calls to the Originating C/CSP or Transit C/CSP.

***Numbering Plan***

means the *Telecommunications Numbering Plan 2015*.

***Originating C/CSP***

means a C/CSP that provides voice telephony call services to an A-Party customer directly connected to the C/CSP.

***Public Number***

means a number specified in the Numbering Plan as referred to in subsection 455(3) of the Act.

***Scam Call***

means any voice telephony call which has been generated for the purpose of dishonestly obtaining a benefit, or causing a loss, by deception or other means.

***Terminating C/CSP***

means a C/CSP that provides voice telephony services to a B-Party customer.

***Transit C/CSP***

means a C/CSP that connects with C/CSPs and International Operators to pass call traffic between them.

***Telecommunications Network***

has the meaning given by section 7 of the Act.

## 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 CONSUMER INFORMATION

#### 3.1 Education about scam calls

- 3.1.1 C/CSPs must make available, including on their websites, up-to-date guidance material for customers which may include:
- (a) the types of Scam Call related fraud risks to which customers may be exposed;
  - (b) information about products or services to assist in blocking suspicious or unwanted international or domestic calls;
  - (c) the steps customers could take to mitigate those risks, such as:
    - (i) protecting their personal information and not sharing it with unknown or unsolicited callers;
    - (ii) contacting their financial institution immediately if they believe they have lost money to a scammer;
    - (iii) changing default PINs and passwords on newly acquired customer equipment;
    - (iv) selecting strong PINS and passwords (e.g. Not "1234" or "0000" or "password" etc.);
    - (v) locking mobile handsets with secure PINs;
    - (vi) ensuring that voicemail PINs are secure;
    - (vii) disabling PABX ports and features that are not used (e.g. remote call-forwarding);
    - (viii) changing PINs and passwords regularly;
    - (ix) not responding to missed calls from unknown international numbers or unknown Australian numbers;
    - (x) blocking suspicious or unknown domestic or international numbers on mobile handsets and use of blocking services or products, where available, on landlines;
  - (d) not responding to SMS from unknown numbers; and
  - (e) the actions that customers should take if they find that they have received Scam Calls such as reporting the scam to [www.Scamwatch.gov.au](http://www.Scamwatch.gov.au) .

*NOTE: [Scamwatch](#), [Stay Smart Online](#) and the [ACMA](#) all provide awareness raising material about scams to consumers, as do other government departments like the Australian Taxation Office and Department of Human Services. The ACCC's [Little black book of scams](#) is one particularly noteworthy and comprehensive example of scam awareness raising.*

## 4 SCAM CALLS

### 4.1 Characteristics of Scam Calls

4.1.1 Scam Calls are often characterised by:

- (a) High volume from a particular CLI or range of CLIs;
- (b) Short duration;
- (c) CLI issues:
  - (i) the A-party CLI does not present to the Terminating C/CSP as a Public Number that can be called back, i.e. there is no way of verifying the originating A-party (for example the call cases where a dummy A-party CLI has been inserted by the Originating C/CSP for compliance with CA G549:2000 Interconnection Implementation Plan & G500:2000 Interconnect Signalling Specification;

*NOTE: At the time of publication of the Code, Communications Alliance working committee WC89 is revising the associated G500:2000 and G549:2000 specifications to align with the clause 4.3.2 requirement.*

- (ii) the CND is blocked;
- (iii) the A-party CLI is from an 'incorrect' number range, i.e. the Originating C/CSP has not been allocated the number range, or the number has not been ported to the Originating C/CSP (see Clause 4.3.1);
- (iv) the A-party CLI of an inbound international call is an Australian number or is not conforming to the ITU-T Recommendation E.164
- (v) the A-Party CLI is a number which is longer than normal and/or is being generated from unallocated number ranges (see Clause 4.3.1);
- (vi) the A-party CLI is not used in accordance with the Numbering Plan i.e. use of 13/1300/1800/1900 numbers as A-Party CLI for outbound calls; and
- (vii) no A-Party CLI has been provided by the International Operator for an inbound international call.

### 4.2 Identifying Scam Calls

4.2.1 As legitimate phone calls (including telemarketing calls) can also exhibit the same characteristics as Scam Calls, further evidence is required to identify Scam Calls. Further evidence can include:

- (a) abnormally high volumes of traffic from a Carriage Service that does not usually generate that volume of traffic in the ordinary usage of that service;

- (b) receiving customer complaints regarding phone calls that appear to be seeking information, for the purposes of committing fraud or where the customer has been scammed;
- (c) customer complaints that their A-Party number has been subject to CLI Spoofing;
- (d) complaints to the regulators about particular A-Party CLI being used for Scam Calls; and
- (e) the CND details are invalid or the number presented as the A-Party CLI is valid but has been subject to CLI Spoofing.

### 4.3 Improving CLI accuracy

- 4.3.1 Originating C/CSPs must only originate calls on their Telecommunications Network with CLIs, in accordance with the Numbering Plan, using the number ranges allocated to them where the numbers are:
  - (a) allocated directly to the Originating C/CSP by the ACMA; or
  - (b) transferred to them via a 3rd party C/CSP contractual relationship; or
  - (c) ported in from another C/CSP.
- 4.3.2 Australian Transit C/CSPs must send the full international CLI of inbound international calls received from the International Operator XPOI to the Transit C/CSPs or Terminating C/CSPs.
- 4.3.3 C/CSPs should not send inbound international calls to B-Parties on their own Telecommunications Network or XPOI to the Transit C/CSPs or Terminating C/CSPs where the A-party CLI of an inbound international call is showing an Australian number, unless the C/CSP is satisfied that use of the Australian number is a genuine call case.
- 4.3.4 C/CSPs must not send calls to B-Parties on their own Telecommunications Network or XPOI to the Transit C/CSPs or Terminating C/CSPs where 13/1300/1800/1900 numbers are being used as A-Party CLI.
- 4.3.5 If a C/CSP identifies a material issue of CLI Spoofing, the C/CSP must raise the issue, as soon as practicable, with the Originating C/CSP or the Transit C/CSP delivering the call traffic for investigation and remediation and should provide details about the Scam Calls (including, where possible, details of the scammers) to the ACMA.
- 4.3.6 Australian Transit C/CSPs must not send calls to B-Parties on their own Telecommunications Network or XPOI to the Transit C/CSPs or Terminating C/CSPs where the A-Party CLI of an inbound international call has either not been provided by the International Operator or is not conforming to the ITU-T Recommendation E.164.

- 4.3.7 Australian Transit C/CSPs must not send calls to International Operators without an A-Party CLI or with a CLI which is not conforming to the ITU-T Recommendation E.164.

#### 4.4 **Monitoring for Scam Calls**

- 4.4.1 C/CSPs must monitor their networks for Scam Calls based upon their characteristics in clauses 4.1 & 4.2 noting that these characteristics are not intended to be exhaustive or restrictive in terms of monitoring that may occur.
- 4.4.2 C/CSPs must monitor their networks for Scam Calls based upon the CLI received from other C/CSPs or from the regulators which are associated with Scam Calls (see Clause 4.4.6).

*NOTE: Each C/CSP is responsible for determining how they monitor their networks to detect Scam Calls on their networks.*

- 4.4.3 A Notifying C/CSP must provide details of the Scam Calls with a material issue, to the Originating C/CSP or Transit C/CSP delivering the Scam Calls for investigation and remediation as soon as practicable, via email, as per the template in Appendix A.
- 4.4.4 Where the Scam Calls are originating from their own directly connected A-Party customers, the C/CSP is responsible for investigation and remediation.
- 4.4.5 C/CSPs must accept and acknowledge receipt of the CLI received from other C/CSPs or from the regulators which are associated with Scam Calls for monitoring in their networks, as soon as practicable.
- 4.4.6 Minimum details of the Scam Calls to be provided to the Originating C/CSP or Transit C/CSP include:
- (a) the date and time (with UTC offset) of the Scam Calls;
  - (b) the CLI used for the Scam Calls;
  - (c) the number of Scam Calls identified in the relevant period; and
  - (d) further evidence if requested by the Originating C/CSP or Transit C/CSP (e.g. customer complaints, call characteristics, CDRs) to support the identified calls as being Scam Calls rather than legitimate calls.

#### 4.5 **Tracing Scam Calls**

- 4.5.1 C/CSPs must cooperate with each other in the prevention, investigation and mitigation of Scam Calls as well as any other Carriage Services used for scams in accordance with sections 279, 287 and 313 (1) of the Act and section 474.17 of the *Criminal Code Act 1995*.
- 4.5.2 Originating C/CSPs or Transit C/CSPs must acknowledge receipt of the evidence provided by the Notifying C/CSP as soon as practicable.

- 4.5.3 When presented with evidence, under Clause 4.4, the Originating C/CSP or the Transit C/CSP must investigate and, where found to be Scam Calls, trace the origin of the Scam Calls as soon as practicable. This includes, if necessary, providing details of the Scam Calls to another Transit C/CSP as soon as practicable.
- 4.5.4 Where a Notifying CSP provides evidence, under Clause 4.4, to another C/CSP about calls that they believe to be Scam Calls, and the other C/CSP does not respond or otherwise does not take the required action under Clause 4.5.3 and Section 4.6, the Notifying C/CSP must inform the ACMA about the matter along with details about the Scam Calls (including, where possible, details of the scammers) as soon as practicable.
- 4.5.5 Following on from clause 4.4.4, a C/CSP must have processes in place to trace the origin of Scam Calls, originating on its own network.
- 4.5.6 Where Scam Calls are confirmed, C/CSPs must as soon as practicable:
- (a) take action to stop the Scam Calls being originated and/or carried over their network as close as possible to the origin of the Scam Calls in accordance with sections 4.6 and 4.7;
  - (b) share information about the origin and transit path of the Scam Calls with other C/CSPs via email; and
  - (c) provide details about the Scam Calls (including, where possible, details of the scammers) to the regulators.

## 4.6 **Blocking Scam Calls**

- 4.6.1 Where reported Scam Calls are confirmed to be Scam Calls, a C/CSP must, as soon as practicable, temporarily or permanently block the Public Number originating the call(s) depending on the origin.
- 4.6.2 C/CSPs must take action to block Scam Calls as close as possible to the origin of the Scam Calls.
- 4.6.3 Blocking of Scam Calls must include blocking incoming calls from and outgoing calls to the Public Number originating the Scam Calls.
- 4.6.4 Where a Public Number is found to be no longer being used for Scam Calls or was incorrectly blocked, a C/CSP must take action to unblock that Public Number as soon as practicable.

## 4.7 **Blocking calls from International Operators**

- 4.7.1 When Scam Calls are identified as originating internationally, C/CSPs must request the assistance of the International Operator in stopping the delivery of further Scam Calls from the identified CLIs into Australia and advise that such Scam Calls are being blocked.
- 4.7.2 C/CSPs must block international Public Numbers found to be originating Scam Calls and not send them to B-Parties on their

own Telecommunications Network or XPOI to the Transit C/CSPs or Terminating C/CSPs.

- 4.7.3 In making a request under 4.7.1, a C/CSP must follow the processes and provide the same information to the International Operator as being provided under clause 4.4.6.
- 4.7.4 If the International Operator does not act to stop the delivery of further Scam Calls from the identified CLIs as soon as practicable of a C/CSP making the request under clause 4.7.1, the C/CSP should issue the International Operator a notice advising that the C/CSPs may introduce temporary blocking of all calls from the International Operator.
- 4.7.5 If the International Operator fails to respond to a notice issued under clause 4.7.4, the C/CSP must advise the ACMA and C/CSPs registered with CA for the purposes of this Code, of the identity of the International Operator.
- 4.7.6 All C/CSPs accepting calls from the International Operator may then commence temporary blocking of all calls from the International Operator in accordance with the processes outlined in clauses 4.7.1 to 4.7.5.
- 4.7.7 Blocking of an International Operator must only occur if the International Operator has failed to satisfactorily respond to a request to stop delivery of further Scam Calls from the identified CLIs.
- 4.7.8 Where an International Operator has been blocked in accordance with clause 4.7.7 but is found to be no longer uncooperative or unresponsive, a C/CSP must take action to unblock that International Operator as soon as practicable and must advise the ACMA and C/CSPs registered with CA for the purposes of this Code, (noting that clause 4.7.2 will still apply).

## 5 C/CSP CONTACT LIST

- 5.1.1 For the purposes of meeting the information sharing and notification obligations under the Code, C/CSPs providing the Carriage Service scoped by the Code must register their contact details with CA.
- 5.1.2 C/CSPs must complete, maintain and keep up to date, an industry contact list and provide their details to CA. C/CSPs must maintain and keep the contacts current.

NOTE: CA will maintain the contact matrix on its website – [www.commsalliance.com.au](http://www.commsalliance.com.au), with updates within 24 hours (one Business Day) of notification of the change. The contact list is password protected.

Example contact list template

Carrier / CSP Name	Phone Contact	Email Contact	1 <sup>st</sup> Level Escalation

## 6 REFERENCES

<b>Publication</b>	<b>Title</b>
<b>Industry Documents</b>	
G549:2000	Interconnection Implementation Plan
G500:2000	Interconnect Signalling Specification for Circuit Switched Networks
<b>Recommendations</b>	
ITU-T E.164	(11/2010)
<b>Legislation</b>	
	<i>Criminal Code Act 1995</i>
	<i>Competition and Consumer Act 2010</i>
	<i>Do Not Call Register Act 2006</i>
	<i>Privacy Act 1988</i>
	<i>Spam Act 2003</i>
	<i>Telecommunications Act 1997</i>
	<i>Telecommunications (Consumer Protection and Service Standards) Act 1999</i>
	<i>Telecommunications Numbering Plan 2015</i>

## APPENDIX

### A Sample for information sharing request

Details of Scam Call(s)	<i>[Dates and times, duration, A-number, associated CLI, number of Scam calls in the relevant period, and if requested the relevant CDRs].</i>
Details of complaints received (if applicable)	<i>[number of complaints, reported loss, timing of complaints]</i>
Validation of CLI used for the Scam Call(s)	<i>[Type and nature of validation checks conducted, e.g. CLI callback, online search yielding evidence of complaints associated with CLI]  [Outcomes of validation checks, e.g. CLI has been used to perpetrate illegitimate calls, CLI has been used legitimately for telemarketing calls, etc]</i>

Select from the following:

*[Notifying C/CSP] requests that [Transit C/CSP] inspect its communications records in relation to Scam Calls detailed above to determine if these are presenting on the Transit C/CSP network.*

*[Transit C/CSP] should inform [Notifying C/CSP] from time to time of the progress of the investigation.*

Contact Name: \_\_\_\_\_

Contact Number: \_\_\_\_\_

Signed: \_\_\_\_\_

Date: \_\_\_\_\_

## **PARTICIPANTS**

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

<b>Organisation</b>	<b>Membership</b>	<b>Representative</b>
ACMA	Non-voting	Bridget Smith
ACMA	Non-voting	John Mullaney
MNF Group	Voting	Geoff Brann
Optus	Voting	Sanjeev Mangar
Optus	Non-voting	Warren Hudson
Pivotel	Voting	Heather Trieu
Telstra	Voting	Tony Rayner
Telstra	Non-voting	John Laughlin
Verizon Australia	Voting	Stephen Mayger
Vocus	Voting	Matthew Crippa
Vocus	Non-voting	Leanne O'Donnell
Vodafone Hutchison Australia	Voting	Alexander R. Osborne

This Working Committee was chaired by John Laughlin. 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](mailto:info@commsalliance.com.au)  
[www.commsalliance.com.au](http://www.commsalliance.com.au)  
ABN 56 078 026 507**

Care should be taken to ensure the material used is from the current version of the Standard or Industry Code and that it is updated whenever the Standard or Code is amended or revised. The number and date of the Standard or Code should therefore be clearly identified. If in doubt please contact Communications Alliance