

**COMMUNICATIONS
ALLIANCE LTD**



INDUSTRY CODE

C661:2020

REDUCING SCAM CALLS

C661:2020 REDUCING SCAM CALLS 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

© 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.

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 and SMS scam traffic.

This Code focuses on Scam Calls as the phone remains the preferred contact method of scammers. However, Communications Alliance is committed to disrupting SMS scams, including working within the ACMA's Scam Telco Action Taskforce to ensure best practice network management (including filtering technology) is implemented.

As the peak communications body Communications Alliance is committed to monitoring international best practice scam mitigation strategies in the context of the Australian environment as part of a continuous improvement model.

This Code sets out processes 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 relevant government agencies.

John Laughlin
Chair

WC92 Reducing Scam Calls Working Committee

NOVEMBER 2020

TABLE OF CONTENTS

1	GENERAL	2
	1.1 Introduction	2
	1.2 Registration by the ACMA	2
	1.3 Scope	3
	1.4 Objective	3
	1.5 Code review	4
2	ACRONYMS, DEFINITIONS AND INTERPRETATION	5
	2.1 Acronyms	5
	2.2 Definitions	6
	2.3 Interpretation	8
3	CONSUMER INFORMATION	9
	3.1 Education about Scam Calls	9
4	SCAM CALLS	10
	4.1 Identifying Scam Calls	10
	4.2 Improving CLI accuracy	11
	4.3 Monitoring for Scam Calls	12
	4.4 Tracing Scam Calls	13
	4.5 Blocking Scam Calls	13
	4.6 Unblocking Public Numbers	14
	4.7 Seeking assistance from International Operators	14
5	C/CSP CONTACT LIST	15
6	REFERENCES	16
	APPENDIX A	17
	APPENDIX B	18
	PARTICIPANTS	19

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 must be read in conjunction with CA G664:2020.

NOTE: G664:2020 is available for Industry participants only.

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 *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. In complying with the Code, C/CSPs will have regard to the protection of communications provisions in the Act and the obligations at 313 (1) of the Act and section 474.17 of the *Criminal Code Act 1995*.
- 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 the Act.
- 1.3.5 The Code applies to Scam Calls which are originated via a Listed Carriage Service.
- 1.3.6 The Code does not apply to Scam Calls that are delivered independently of a Carrier's or CSP's voice telephony switches (e.g. 'over the top' of a mobile data service).

1.4 Objective

- 1.4.1 The objective of the Code is to disrupt scam activity by:
 - (a) defining Scam Calls in the context of the Code;
 - (b) establishing processes by which C/CSPs will work with each other and relevant government agencies to identify and handle Scam Calls;
 - (c) establishing processes to share and communicate evidence of Scam Calls between C/CSPs and relevant government agencies;
 - (d) establishing processes for C/CSPs to exchange information in order to trace the origin of Scam Calls;
 - (e) establishing a process for C/CSPs to Block Scam Calls (from specific A-Party CLI(s)); and
 - (f) establishing 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.

2 ACRONYMS, DEFINITIONS AND INTERPRETATION

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.

CLIR

means Calling Line Identification Restricted.

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.

Block

means to stop or otherwise disrupt the delivery of calls.

NOTE: Blocking can apply to incoming calls from and outgoing calls to the Public Number or International Number originating the calls.

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 Restriction

has the meaning given by G500:2020.

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.

Inbound International Calls

means calls originating outside of Australia.

International Number

has the meaning given in the Numbering Plan.

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.

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.

Telecommunications Network

has the meaning given by section 7 of the Act.

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.

2.3 Interpretation

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 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 or SMS from unknown International Numbers, unknown Australian numbers or an unknown source;
 - (x) Blocking suspicious or unknown domestic or International Numbers on mobile handsets and use of Blocking services or products, where available, on landlines;
 - (xi) allowing unknown calls to go to voicemail and then listening to any message left to ascertain if this might be a genuine call.
 - (d) 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 .

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 Identifying Scam Calls

4.1.1 Scam Calls are often characterised by:

- (a) High volume from a particular CLI or range of CLIs;

NOTE: High volume calls are not the primary evidence that the calls originating from an individual number are Scam Calls.

- (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 G549:2020 Interconnection Implementation Plan & G500:2020 Interconnect Signalling Specification;
- (ii) the CND is Blocked with CLI Restriction;
- (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 (see CA G664:2020 for examples) 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; and
- (vii) no A-Party CLI has been provided by the International Operator for an Inbound International Call.

4.1.2 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;

NOTE: High volume calls are not the primary evidence that the calls originating from an individual number are Scam Calls.

- (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 relevant government agencies 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.

4.2 Improving CLI accuracy

Domestically Originated Calls

- 4.2.1 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; or
 - (d) issued to the A-Party caller by the Originating C/CSP; or
 - (e) allocated to an entity the Originating C/CSP has a domestic or international roaming agreement with.
- 4.2.2 Clause 4.2.1 does not impose any A-Party CLI accuracy validation requirements on Transit C/CSPs and Terminating C/CSPs for calls:
 - (a) which are received XPOI from Originating C/CSPs and/or Transit C/CSPs;
 - (b) which are received via call redirection or call forwarding from a B-Party.
- 4.2.3 Australian Transit C/CSPs must not send calls to International Operators without an A-Party CLI.
- 4.2.4 Australian Transit C/CSPs must not send calls to International Operators with a CLI which is not conforming to the ITU-T Recommendation E.164 unless the CLI is associated with an international inbound mobile roaming service.

Internationally Originated Calls

- 4.2.5 Australian Transit C/CSPs must send the international CLI of Inbound International Calls as received from the International Operator XPOI to the Transit C/CSPs or Terminating C/CSPs.

*NOTES: 1. See CA G549:2020 Interconnection Implementation Plan & G500:2020 Interconnect Signalling Specification for CLI compliance.
2. Where the A-Party CLI does not conform to the ITU-T Recommendation E.164, then these calls should be subject to scrutiny as potential Scam Calls.*

- 4.2.6 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 exceptions apply (as per CA G664:2020).
- 4.2.7 Australian Transit C/CSPs must not send calls XPOI to the Transit C/CSPs or Terminating C/CSPs where the A-Party CLI of an Inbound International Call has not been provided by the International Operator.

All Calls

- 4.2.8 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.
- 4.2.9 If a C/CSP identifies a material issue of alleged 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 to undertake appropriate action to Block the Scam Calls.
- 4.2.10 The Notifying C/CSP in clause 4.2.9 should provide details about the alleged Scam Calls (including, where possible, details of the scammers) via email to the ACMA as per the template in Appendix B.

4.3 Monitoring for Scam Calls

- 4.3.1 C/CSPs must monitor their networks for Scam Calls based upon their characteristics in sections 4.1 & 4.2 noting that these characteristics are not intended to be exhaustive or restrictive in terms of monitoring that may occur.

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

- 4.3.2 C/CSPs must monitor their networks for Scam Calls based upon the CLI notified by other C/CSPs or from relevant government agencies which are associated with Scam Calls (see Clause 4.3.4).
- 4.3.3 A Notifying C/CSP must provide details of the alleged Scam Calls with a material issue, to the Originating C/CSP or Transit C/CSP

delivering the alleged Scam Calls, for investigation as soon as practicable, via email, as per the template in Appendix A.

- 4.3.4 C/CSPs must accept and acknowledge via email, receipt of the reports of CLI notified by other C/CSPs or from relevant government agencies which are associated with alleged Scam Calls for monitoring in their networks, as soon as practicable.
- 4.3.5 Minimum details of the alleged Scam Calls to be provided to the Originating C/CSP or Transit C/CSP must include:
 - (a) the date and time (with UTC offset) of the alleged Scam Calls;
 - (b) the CLI used for the alleged Scam Calls;
 - (c) the number of alleged 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 alleged Scam Calls rather than legitimate calls.

4.4 Tracing Scam Calls

- 4.4.1 A C/CSP must have processes in place to trace the origin of alleged Scam Calls, originating on its own network.
- 4.4.2 In accordance with the protection of communications provisions of the Act and the obligations at section 313(1) of the Act and section 474.17 of the Criminal Code Act 1995, C/CSPs must cooperate with each other in the prevention, investigation and mitigation of scams which are using their Carriage Services, whether a Scam Call or a scam perpetrated by other means.
- 4.4.3 When presented with evidence, under section 4.3, 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.
- 4.4.4 Where a Notifying CSP provides evidence, under Clause 4.3.3, 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 4.4.3 and section 4.5, the Notifying C/CSP must inform the ACMA via email, as per the template in Appendix B, about the matter along with details about the alleged Scam Calls (including, where possible, details of the scammers) as soon as practicable.

4.5 Blocking Scam Calls

- 4.5.1 Where Scam Calls are confirmed, C/CSPs must as soon as practicable take action to Block the Scam Calls being originated and/or carried over their network in accordance with this section (unless the C/CSP has evidence that the Public Number has been subject to CLI Spoofing).

- 4.5.2 Where Scam Calls are confirmed, each C/CSP in the transit path must:
- (a) share information about the origin of the Scam Calls with other C/CSPs via email; and
 - (b) provide details about the transit path of the Scam Calls (including, where possible, details of the scammers) to relevant government agencies via email, as per the template in Appendix B.
- 4.5.3 C/CSPs are responsible for investigating, and undertaking appropriate action to Block the Scam Calls originating from their own directly connected A-Party customers. This may include the disconnection of the A-Party customer's service.
- 4.5.4 Where a C/CSP has detected Scam Calls based upon certain characteristics after considering clause 4.1.1 and clause 4.1.2, it must Block the Public Number or International Number.

NOTE: An example of these types of Scam Calls includes, but is not limited to, Wangiri calls.

- 4.5.5 C/CSPs must Block International Numbers found to be originating Scam Calls and not send the Scam Calls to B-Parties on their own Telecommunications Network or XPOI to the Transit C/CSPs or Terminating C/CSPs.

4.6 Unblocking Public Numbers

- 4.6.1 Where a Public Number is found to be no longer being used for Scam Calls or was subject to CLI Spoofing, a C/CSP should take action to unblock that Public Number as soon as practicable.
- 4.6.2 Where a Public Number is found to be incorrectly Blocked a C/CSP must take action to unblock that Public Number as soon as practicable.

4.7 Seeking assistance from International Operators

- 4.7.1 When a material number of Scam Calls are identified as originating internationally, C/CSPs must use all available contractual arrangements to secure the assistance of the relevant International Operator in stopping further Scam Calls from the identified CLIs into Australia and advise that such Scam Calls are being Blocked.

5 C/CSP CONTACT LIST

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

NOTE: CA will maintain the contact matrix on its website – 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 st Level Escalation

6 REFERENCES

Publication	Title
Industry Documents	
G549:2020	Interconnection Implementation Plan
G500:2020	Interconnect Signalling Specification for Circuit Switched Networks
G664:2020	Reducing Scam Calls – Supplementary Information
Recommendations	
ITU-T E.164	(11/2010)
Legislation	
	<u>Criminal Code Act 1995</u>
	<u>Competition and Consumer Act 2010</u>
	<u>Do Not Call Register Act 2006</u>
	<u>Privacy Act 1988</u>
	<u>Telecommunications Act 1997</u>
	<u>Telecommunications (Consumer Protection and Service Standards) Act 1999</u>
	<u>Telecommunications Numbering Plan 2015</u>

APPENDIX A

Sample for information sharing request between C/CSPs

Details of Scam Call(s)	<i>[Dates and times, duration, A-Party 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: _____

APPENDIX B

Sample for information sharing request between C/CSPs and relevant government agencies

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]</i> <i>[Outcomes of validation checks, e.g. CLI has been used to perpetrate illegitimate calls, CLI has been used legitimately for telemarketing calls, etc]</i>

Contact Name: _____

Contact Number: _____

Signed: _____

Date: _____

PARTICIPANTS

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

Organisation	Membership	Representative
Australian Communications and Media Authority (ACMA)	Non-voting	Bridget Smith
ACMA	Non-voting	John Mullaney
Australian Mobile Telecommunications Assoc. (AMTA)	Non-voting	Lisa Brown
MNF Group	Voting	Geoff Brann
Optus	Voting	Sanjeev Mangar
Optus	Non-voting	Warren Hudson
Pivotel	Voting	Lachlan Highett
Telstra	Voting	Tony Rayner
Telstra	Non-voting	John Laughlin
TPG Telecom Limited	Voting	Alexander R. Osborne
Verizon Australia	Voting	Stephen Mayger
Vocus	Voting	Leanne O'Donnell
Vocus	Non-voting	Matthew Crippa

This Working Committee was chaired by John Laughlin of Telstra. 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**

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