

**COMMUNICATIONS
ALLIANCE LTD**



**INDUSTRY GUIDANCE NOTE (IGN 009)
CLI MANAGEMENT**

CLI Management Industry Guidance Note IGN 009

Disclaimers

1. Despite anything contained in this Guidance Note:
 - (a) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct, indirect or consequential loss, damage, claim, or liability any person may incur as a result of any:
 - (i) reliance on or compliance with this Guidance Note;
 - (ii) inaccuracy or inappropriateness of this Guidance Note; or
 - (iii) inconsistency of this Guidance Note with any law, Industry Code or Industry Guideline; 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 Guidance Note.
2. For avoidance of doubt:
 - (a) You must not rely on the information in this document as an alternative to legal advice from your solicitor or other professional legal services provider.
 - (b) You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information in this document.
3. These 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.

VERSION HISTORY

This document constitutes: Version 1 of Industry Guidance Note IGN 009

Date	Version	Comments/Changes
12/10/2015	1	First release
7/12/2016	2	Second release
23/12/2020	3	Third release to align with industry code C661 Reducing Scam Calls.

TABLE OF CONTENTS

1	BACKGROUND	5
2	OBJECTIVE OF THIS GUIDANCE NOTE	5
3	ABOUT CLI AND CLI SPOOFING	6
	3.1 What is CLI?	6
	3.2 What is CLI Spoofing?	6
4	REGULATORY REQUIREMENTS	6
5	INTERCONNECTED NETWORKS AND CLI	7
6	CLI MANAGEMENT ISSUES	7
	6.1 What is CLI Management?	7
	6.2 Who replaces the CLI?	7
	6.3 Is CLI Management permitted?	8
	6.4 CLI Spoofing	9
	6.5 What can a C/CSP do about CLI Spoofing?	9
7	OTHER CONSIDERATIONS	10
	7.1 Emergency calling	10
	7.2 Issues with some VOIP services	10
8	REFERENCE DOCUMENTS	11
	APPENDIX	12
A	PART 18 OF THE TELECOMMUNICATIONS ACT 1997	12
	APPENDIX	13
B	ADMA CODE OF PRACTICE	13

1 BACKGROUND

Carriers and Carriage Service Providers (CSPs) in the telecommunications industry use Calling Line Identification (CLI) for the routing of telephone calls (e.g., for inbound calls) and billing of services. Billing applies to both interconnected services between carrier and CSP networks and to end user billing (e.g., for pre-selected services and premium services).

CLI is also used as a basis for Calling Number Display (CND) for end users and for meeting carrier & CSP obligations relating to law enforcement and national security matters such as lawful interception and data retention.

Accurate CLI is important for the effective operation of carrier & CSP networks. In some cases, the CLI may be changed for legitimate business practices. However, the CLI may also be changed for illegal or fraudulent purposes (this is generally referred to as CLI spoofing.) This is a serious concern to carriers and CSPs as it affects their customers.

2 OBJECTIVE OF THIS GUIDANCE NOTE

This industry guidance note has been prepared to give information on the nature and handling of CLI. It is intended to help clarify the range of uses and abuses of CLI, and outline some of the practices in industry. In particular, it provides advice for carriers and CSPs on how to tackle the practice of CLI spoofing. The overall objective is that end customers making calls across networks can be uniquely identified by the CLI presented.

This industry guidance note may also be of use to Emergency Service Organisations (ESOs), which require on accurate CLI to help them respond to emergency calls.

3 ABOUT CLI AND CLI SPOOFING

3.1 What is CLI?

- 3.1.1 CLI means the data generated by a Telecommunications Network which relates to the Public Number of the A-Party.
- 3.1.2 CLI is used by carrier & CSP networks to accurately route calls between networks and to deliver calls to the receiving network or end user.
- 3.1.3 CLI is also used by billing systems to accurately rate calls.
- 3.1.4 An originating carrier or CSP should assign a CLI that matches the relevant public number(s) issued to the calling customer from which the call originates.

3.2 What is CLI Spoofing?

- 3.2.1 CLI spoofing means the unauthorised use of a public number, 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.

4 REGULATORY REQUIREMENTS

- 4.1.1 The *Telecommunications Act 1997 (Act)* provides only brief information regarding CLI. Part 18 of the *Act* requires that “a switching system used in connection with the supply of a standard telephone service ... is capable of providing calling line identification”.

NOTE: Refer to Appendix A for more information on Part 18.

In Part 18, the reference to a “switching system used in connection of a standard telephone service” would originally have been a ‘PSTN Local Access Switch or its equivalent’ but now several different platform are used to provide voice calls. These include the National Broadband Network (NBN), DSL Access Networks and emerging 4G LTE mobile networks – where voice is an application on an underlying data network.

- 4.1.2 The other reference to CLI is in the *Act* Part 6, Section 125A where it is required that the ACMA determine a standard that ensures that CLI is provided in respect of telemarketing calls.
- 4.1.3 The *Numbering Plan 2015* is also relevant. Section 16 covers the numbers in use and states that no other number may be used in connection with the supply of carriage services to the public in Australia.
- 4.1.4 Communications Alliance industry code C525 Handling of Life Threatening and Unwelcome Communications contains obligations on Access service providers to trace back nuisance communications to the source. Accurate CLI is essential for this process to work effectively across networks.

- 4.1.5 Communications Alliance industry code C661 Reducing Scam Calls places obligations on C/CSPs to reduce scam calls, by requiring CLI accuracy and usage in accordance with the code rules.

5 INTERCONNECTED NETWORKS AND CLI

- 5.1.1 CLI is passed across interconnected carrier & CSP networks via a signalling system. Traditionally this has been defined in interconnect agreements by the C7 signalling standard specified in G500 specification and the CLI structure is defined in G549 specification.
- 5.1.2 However, carriers & CSPs can agree on a bilateral basis to use other interconnecting technologies and signalling systems, a common option being used by "IP" networks is the Session Initiation Protocol (SIP). This allows greater flexibility in the way CLI can be handled.
- 5.1.3 G549 & G500 specifications have been updated in 2020 to require that all interconnected carrier & CSP networks must pass the full international CLI for incoming international calls instead of using a dummy CLI.
- 5.1.4 Networks interconnecting telephone calls originating in Australia should present CLI in accordance with the CLI requirements in industry code C661. Calls without CLI will be blocked by carriers & CSPs in accordance with the requirements of the industry code C661.

6 CLI MANAGEMENT ISSUES

6.1 What is CLI Management?

- 6.1.1 'CLI Management' occurs where the CLI provided with a call is replaced with another CLI that does not match the number(s) issued to the calling customer. This practice is also called 'CLI over stamping'.

6.2 Who replaces the CLI?

- 6.2.1 The deliberate insertion of a different CLI can occur at the point of the originating call, the originating carrier or CSP and/or a transit carrier or CSP.
- 6.2.2 Once a different CLI is inserted, it can pass through the interconnected carrier and CSP networks unless it is detected as invalid by an interconnecting or transit carrier or CSP network, in which case a call attempt would fail.
- 6.2.3 Generally, a changed CLI will only be detected if it is not in accordance with the Numbering Plan, has not been conditioned by CSPs or is not a dummy CLI in accordance with G549 specification.

6.3 Is CLI Management permitted?

- 6.3.1 Sometimes there is a legitimate use for CLI translation (e.g. telemarketing, outbound customer support, large organisations) which will display the call centre or business number rather than an individual extension number.
- 6.3.2 This legitimate use is consistent with the CLI requirements in industry code C661.
- 6.3.3 Accurate CLI is important for reconciling interconnect payments between carrier and CSP networks.
- 6.3.4 Premium rate services need an accurate CLI for billing purposes.
- 6.3.5 Insertion of a 'Dummy' CLI is another example of valid use in carrier and CSP networks to reduce the risk of call failure. The use of dummy CLIs for interconnecting networks is defined in G500 and G549 specifications for certain call cases.
- 6.3.6 Another valid use of a dummy CLI is when a call is made to 000 or 112 from a public mobile telecommunications service where the network is unable to identify the subscriber, such as when the call is made from a handset with no or an inactive SIM or when the handset is emergency camped on a mobile network other than its home mobile network. In these cases, the mobile carriers have a set range of numbers that are used and known to the Emergency Call Person and ESOs (i.e., police, fire and ambulance services).
- 6.3.7 Communications Alliance maintains, on its website, an industry list of dummy CLIs that is available to authorised users– typically those requiring the information for accurate call routing purposes and ESOs.
- 6.3.8 There are also appropriate business circumstances where the original CLI may be substituted with a more useful CLI (also a legitimate issued number to the calling party). An example of acceptable practice is included in the Association for Data-Driven Marketing & Advertising (ADMA) Direct Marketing Code of Practice¹, which recommends the CLI transmitted should be a "*telephone number which is suitable for return telephone contact for an individual*".
- 6.3.9 It is not acceptable to use one or a pool of dummy CLIs simply because the originating carrier or CSP has not made the effort to issue numbers to customers, i.e., it has not complied with the Numbering Plan, and/or does not meet the basic requirement of the legislation to supply CLI and/or does not comply with the CLI requirements in industry code C661.

¹ <https://www.adma.com.au/compliance/code-of-practice>

6.4 CLI Spoofing

- 6.4.1 There are situations where CLI Spoofing could threaten the integrity of network routing and impact on customers receiving the call. For example, where threatening or nuisance calls to an individual or nuisance calls to emergency services are made.
- 6.4.2 It is important to differentiate this from appropriate business use as indicated above in Section 6.3.

6.5 What can a C/CSP do about CLI Spoofing?

- 6.5.1 All carriers and CSPs are obliged to comply with legislation, for example, section 355 in Part 18 of the Act and with the ACMA registered industry codes C525 & C661.

NOTE: Part 18 of the Act is more concerned with the ability to provide CLI rather than addressing how it may be used, adjusted or changed and hence does not assist greatly in addressing CLI Spoofing.

- 6.5.2 If a carrier or CSP identifies a potential issue of CLI spoofing, it should be highlighted with the end user, wholesale customer or interconnected carrier or CSP concerned, via normal operational interfaces.
- 6.5.3 This industry guidance note and industry code C661 are considered as the first steps in addressing CLI Management. Consideration will be given to producing in the future the following information:
 - (a) Rules in the Numbering Plan for all C/CSPs that are allocated numbers from the ACMA (medium term) to respect and protect the originating CLI.
 - (b) Representation at International ITU-T numbering and other international Standards forums to address unauthorised use or change of numbers to disguise the originating CLI.

7 OTHER CONSIDERATIONS

7.1 Emergency calling

- 7.1.1 An ESO requires an accurate CLI to enable the ESO to call back the emergency caller in the event that the emergency call drops out. The source of nuisance calls to the emergency number and callers making false emergency reports also needs to be accurately determined.
- 7.1.2 Law enforcement agencies also require an accurate CLI for law enforcement purposes.
- 7.1.3 As noted above, an exception exists for calls made to 000 or 112 from a public mobile telecommunications service where the network is unable to identify the service as it is not native to that network.
- 7.1.4 It is also noted that there are situations where the CLI provided on the call is not a reliable indicator of the calling party's location, e.g., out of area local numbers and services connected to a private exchange that may terminate in a different location to the private exchange. In this case, data is provided to the IPND by way of a unique flag to indicate this lack of location reliability.

7.2 Issues with some VOIP services

- 7.2.1 Some voice telephony services originate on the internet and connect via a gateway to carrier and CSP networks. Such voice telephony services nevertheless are carriage services that:
 - (a) are covered by the Numbering Plan;
 - (b) are subject to the Numbering Plan; and
 - (c) have the requirement in section 462 (1) of the Act to comply with the Numbering Plan.
- 7.2.2 Where these services do not meet regulatory requirements (e.g., the *Numbering Plan*), the call should not progress to the destination if the CLI would deceive the receiving end-user of the caller's identity, including the Emergency Call Person and ESOs as end users.
- 7.2.3 Enforcement for interconnecting VoIP service providers is based on compliance with the requirements of section 462 (1) of the Act i.e., to comply with the *Numbering Plan*.
- 7.2.4 A carrier or CSP might experience a VoIP Distributed Denial of Service (DDOS) attack on emergency calls and the carrier or CSP cannot trace the caller.
- 7.2.5 A lack of a traceable CLI on calls to emergency services makes it difficult for carriers and CSPs to resolve the nuisance call problem.
- 7.2.6 Further disturbing evidence shows that while the industry is attempting to combat the issue, there are software applications becoming readily available to the general public that openly promote CLI Spoofing.

8 REFERENCE DOCUMENTS

TABLE 1
Reference Documents

Legislation	Title
	Telecommunications Act 1997 http://www.comlaw.gov.au/Series/C2004A05145
Regulatory Arrangements	
	Numbering Plan 2015 http://www.comlaw.gov.au/Series/F2015L00319
Communications Alliance documents	
G522:2016	Calling Number Display http://www.commsalliance.com.au/Documents/all/guidelines/g522
C525:2017	Handling of Life Threatening and Unwelcome Communications http://www.commsalliance.com.au/Documents/all/codes/c525
C554:2004	Rights of Use of Premium Rate Service Numbers http://www.commsalliance.com.au/Documents/all/codes/c554
C566:2005	Rights of Use of Numbers https://www.commsalliance.com.au/Documents/all/codes/c566
G500:2020	Signalling System No. 7 - Interconnection ISUP http://www.commsalliance.com.au/Documents/all/Specifications/G500_2000
G549:2020	Interconnection Implementation Plan http://www.commsalliance.com.au/Documents/all/Specifications/G549_2000
C661:2020	Reducing Scam Calls Communications Alliance - C661:2020 Reducing Scam Calls (commsalliance.com.au)

APPENDIX

A PART 18 OF THE *TELECOMMUNICATIONS ACT 1997*

Part 18—Calling line identification

354 Simplified outline

The following is a simplified outline of this Part:

- Certain switching systems must be capable of providing calling line identification.

355 Calling line identification

- (1) This section applies to a person if:
- (a) the person is a carrier or a carriage service provider; and
 - (b) a controlled facility of the person consists of:
 - (i) a switching system used in connection with the supply of a standard telephone service; or
 - (ii) a switching system of a kind specified in a determination under subsection (3); and
 - (c) either:
 - (i) the completion of the installation of the system occurred on or after 1 July 1997; or
 - (ii) immediately before 1 July 1997, the system was capable of providing calling line identification.
- (2) The person must take all reasonable steps to ensure that the system is capable of providing calling line identification.
- (3) The ACMA may, by legislative instrument, make a determination for the purposes of subparagraph (1)(b)(ii).

356 Exemptions from calling line identification requirement

- (1) The ACMA may, by notice in the Gazette, declare that a specified person is exempt from the requirement set out in section 355. The declaration has effect accordingly.

Note: A person may be identified by name, by inclusion in a particular class or in any other way.

- (2) In deciding whether a person should be exempt from the requirement set out in section 355, the ACMA must have regard to the following matters:
- (a) whether it would be unreasonable to impose the requirement;
 - (b) whether it is in the public interest to impose the requirement.
- (3) Subsection (2) does not, by implication, limit the matters to which the ACMA may have regard.

APPENDIX

B ADMA CODE OF PRACTICE

Extract from the ADMA Code of Practice on Calling line identity (CLI):

10 When making an outbound telemarketing call, Members must not block the transmission of the CLI to any calling number display or any calling name display of a consumer who receives the Telephone calls.

11 Where technically feasible, Members should ensure that when outbound calls are made from within the organisation, the number which is transmitted or displayed on receiver terminals is a telephone number which is suitable for return telephone contact by an individual.

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
TTY 61 2 9923 1911
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