COMMUNICATIONS ALLIANCE LTD

# INDUSTRY CODE

# C525:2023 Incorporating Amendment No.1 2024

# HANDLING OF LIFE THREATENING AND UNWELCOME COMMUNICATIONS

**C525:2023 Incorporating Amendment No.1 2024 Handling of Life Threatening and Unwelcome Communications Industry Code**

First published as ACIF C525:1999
Second edition as ACIF C525:2002
Third edition as ACIF C525:2005
Fourth edition as ACIF C525:2006
Fifth edition as C525:2009
Sixth edition as C525:2010 (February 2010)
Seventh edition as C525:2017
Eighth edition as C525:2017 Incorporating Variation No.1/2018

**Communications Alliance Ltd (formerly Australian Communications Industry Forum Ltd) was formed in 2006 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 C525:2023 Incorporating Amendment No.1 2024 ***Handling of Life Threatening and Unwelcome Communications*** Industry Code.

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

The **Handling of Life Threatening and Unwelcome Communications** Code is designed to provide a standard procedure for the cooperative handling, including Communications Tracing, by Suppliers and the National Relay Service Provider (NRSP) of communications which traverse the network(s) of one or more Suppliers and are connected with Life Threatening Communications or a Pattern or Specified Number of Unwelcome Communications.

## Background

In general, Unwelcome Communications are unsolicited communications that, by virtue of the content, frequency or timing, are offensive or tend to menace and harass the recipient. A Life-Threatening Communication is more serious and involves the use of a Carriage Service connected with an event which gives a person reasonable grounds to believe that there is a serious threat to a person's life or health.

To be better able to assist the community and customers, Carriers, Carriage Service Providers (C/CSPs) and Electronic Messaging Service Providers (EMSPs) need to be able to resolve issues of Unwelcome Communications and to provide assistance in life or health threatening situations in an efficient and expedient manner. This means that telecommunications consumers can be assured that there will be a quick response in life or health threatening situations and Unwelcome Communications they may receive will be resolved in a consistent manner with recourse to Police only when the situation warrants it.

Law enforcement agencies and the telecommunications industry recognise the need for an Industry Code that would supplement the existing legislation and establish benchmarks for the satisfactory resolution of Unwelcome Communications and Life-Threatening Communications.

The Code does not apply to the following requests made by law enforcement agencies:

- information under Chapter 4, Part 4-1, Division 4 of the *Telecommunications (Interception and Access) Act 1979*, or
- emergency telecommunications interception under section 30 of the *Telecommunications (Interception and Access) Act 1979*.

In January 1999 the Australian Communications Industry Forum (ACIF) published ACIF C525:1999 ***Handling of Life Threatening and Unwelcome Calls*** Industry Code. The Australian Communications Authority subsequently registered the Code on 27 October 1999.

## 2002 Revision

In the 2002 revision, the Code provided the following additional benefits:

- inclusion of the NRSP;
- accommodation of new telecommunications services such as internet and Short Message Service (SMS) that are being used to make Life Threatening Communications and Unwelcome Communications;
- incorporation of requirements of the Australian Communications Authority's booklet, Developing Telecommunications Codes for Registration – A Guide, which was published after the first version of the Code; and
- resolution of some inconsistencies evident in the first version of the Code.

## 2005 Revision

The 2005 version addressed issues that had emerged, including:

- providing guidance about the particular circumstances in which a C/CSP can deal with unwelcome call complaints relating to non-real time communications (e.g., SMS, Multimedia Message Service (MMS), email);
- specifically including some IP telephony as a Telecommunications Service for the purposes of this Code by including a Standard Telephone Service (STS) in the definition of telecommunications service; and
- modifying the definition of a Pattern of Unwelcome Communications to include unanswered calls and situations when ten or more calls are received within a 24-hour period.

Intercarrier discussion had clarified that there is limited ability to clearly identify all participants in non-real-time communications and that there are jurisdictional limitations that may prevent resolution. As such, the Code was revised to match the capacity of C/CSPs in relation to non-real-time communications, such as SMS, MMS and email. The Communications Service Identification (CSI) information of the originating Carriage Service may not be delivered to the Australian C/CSP and/or may not uniquely identify the originating communications service identifier making it impossible to investigate without the full cooperation of all telecommunications service Suppliers involved in the carriage of the communication and the CSP supplying Carriage Service to the originator of the communication.

C/CSPs must assist end users in receipt of unwelcome messages where it is reasonably possible to do so (e.g., an SMS sent from a mobile handset associated with a Public Number). End users also have a number of options to block or not to read unwelcome messages – unlike traditional voice calls, messages are not delivered as real time communications, and they arrive with the CSI of the originator of the SMS displayed as part of the message. As such, this Code obliges C/CSPs to take action in relation to unwelcome SMS, MMS where it is possible and reasonable to do so.

There are specific instances which are excluded from requirements in the investigation of Unwelcome Communications. For example, when an SMS/MMS is sent from a mobile handset without a Public Number, the name and address details lie with the C/CSP overseas that has the commercial relationship with the originator of the SMS/MMS.

The 2005 Report to the Minister for Communications, Information Technology and the Arts, *Examination of Policy and Regulation Relating to Voice Over Internet Protocol (VoIP)*

*Services* suggested that ACIF Codes might be reviewed for their applicability to VoIP services. The Code revision Working Committee included VoIP calls that conform to the definition of an STS in the Code through the use of the term STS in the definition of telecommunications services that are covered by the Code. VoIP terminals that conform to the STS definition have an allocated Public Number and Unwelcome Communications complaints involving these terminals can be actioned through the C/CSP in the same way as circuit switched telephone calls.

VoIP calls that do not conform to the definition of an STS do not necessarily have an allocated Public Number, and therefore are much more difficult to be successfully investigated by C/CSPs. The electronic address of a VoIP call that is not an STS may only be an IP address. Emails can be traced through their IP address; because emails are a 'store and forward' form of communication the email is delivered to a mail server, where it is recorded before being passed on to the recipient. Non-STS VoIP calls, however, are not a store and forward form of communication: they are near instantaneous communications, delivered into the network as simply a stream of data and the discrete voice 'call' would not necessarily be separately recorded, and therefore not easily investigated.

The revision of the Code moved the definition of a 'Pattern' of Unwelcome Communications to the definitions section.

Other changes made in the 2005 revision of the Code included:

- a requirement that, if the calling party's C/CSP has been advised that Unwelcome Communications have not stopped following receipt of two warning letters, the calling party's C/CSP must Suspend the calling party's telecommunications service;
- clarification as to when the called party/s C/CSP classifies the complaint as an Unwelcome Communication complaint that must be dealt with;
- clarification that complaints concerning telemarketing by or on behalf of an Australian C/CSP are dealt with under the *Privacy Act 1988* and can also be handled by the TIO;
- expansion on advice given to the called party on steps they can take for unwelcome SMS or emails;
- inclusion of zero rated or unanswered calls as calls that can form part of a Pattern of Unwelcome Communications; and
- accommodation of the NRSP if it provides an internet relay service to enable a person who is deaf or has a hearing or speech impairment to communicate in text via the internet while a relay officer uses voice or text to communicate with the other party.

## 2009 Revision

The 2009 version addressed issues that emerged, including:

- updating references to reflect legislative changes;
- modifying the definitions of Unwelcome Communications or Life-Threatening Communications to cover all forms of communications technology subject to the Act;

- clarifying the intent on the handling of Life-Threatening Communications and Unwelcome Communications to multiple Carriage Services of the same entity, from one or more Carriage Services used by the A-Party;
- clarifying intercarrier processes for communications that involve more than two CSPs;
- reflecting changing industry processes as well as the development of new and emerging technologies;
- clarifying the intent on collections and debt recovery practices;
- clarifying the timing and use of warning letter(s);
- supporting industry efforts to reduce non-genuine calls from a public mobile telecommunications service to the Emergency Call Service;
- adding a requirement to provide information for industry contact lists; and
- adding other processes.

A consequence of the above resulted in the change of the name of the Code to the Handling of Life Threatening and Unwelcome Communications Industry Code.

## 2010 Revision

The February 2010 version:

- clarified the handling of Life-Threatening Communications in relation to section 287 of the *Telecommunications Act 1997*;
- clarified the handling of non-genuine calls to Emergency Call Services; and
- editorial changes including to:
- closer align clause 1.1.2 with the wording of section 287 of the Act; and
- add in clause 1.3.1 sections of the industry that reflect existing obligations in the Code.

## 2017 Revision

The 2017 version addressed:

- Patterns of Unwelcome Communications from a single A-Party using multiple communications paths to the same B-Party;
- the need for rules and procedures for managing Unwelcome Communications to Helplines, by adding a new section; specifically, for Helplines;
- handling Unwelcome Communications via an Over-The-Top service;
- changes to reflect industry processes for improved management of Life Threatening and Unwelcome Communications as well as the development of new and emerging technologies; and
- the need to clarify some of the existing Code content and greater clarity around the processes by inclusion of additional notes and flowcharts.

In conjunction with this revision, two Industry Guidance notes were developed. The first is a guide for Customers and the second sets out the agreed thresholds for complaints to Helplines.

## 2018 Variation

Following the registration and implementation of the 2017 Code, minor changes to the practical application of processes in section 4 and section 5 were identified.

The changes in this variation were:

- Parties must consult with the Helpline if they wish to deviate from any processes under section 5 and establish there is no objection from the Helpline to the process deviation. (i.e., if the Helpline objects, the A-Party must continue to adhere to the process under the Code).

- Warning letter templates have been updated advising the point of contact, if there is a dispute, for the relevant Helpline dispute resolution area.

- An action request from the B-Party to the A-Party must include the Helpline's dispute resolution contact details (for the A-Party to include in the letter).

- Supplier obligations given greater clarity and made more consistent between handling general Unwelcome Communications and Unwelcome Communications received by a Helpline.

## Current Regulatory Arrangements

While legislation provides protection against communications that are menacing, harassing or offensive under section 474.17 of the *Criminal Code* within the Criminal Code *Act 1995*, C/CSPs have found that in most cases these issues can be satisfactorily resolved without recourse to Police.

C/CSPs have a general obligation under Part 14 of the *Telecommunications Act 1997* (the Act) to do their best to prevent telecommunications networks and facilities from being used to commit offences and C/CSPs must give authorities such help as is reasonably necessary to enforce the law.

Under section 287 of Part 13, the Act Division 2 (disclosure/use offences) does not prohibit a C/CSP from disclosure or use of customer information where the Supplier believes on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious threat to the life or health of a person.

Disclosure of Customer information should be the minimum amount necessary for the purposes of managing life threatening or unwelcome communications under this Code.

## How the Code Builds on and Enhances the Current Regulatory arrangements

The original Code built on and enhanced the legislation by providing a standard approach for dealing with Unwelcome Communications and Life-Threatening Communications, including the following obligations which have been retained:

- consistency of analysis and management of communications;

- obligations for record keeping on C/CSPs;

- single point of contact for Police in a situation involving a Life-Threatening Communication – available 24 hours a day 7 days a week;
- ensuring central points of contact; and
- obligations on C/CSPs to maintain accuracy and timeliness of contact information.

Subsequent revisions of the Code have included the NRSP in the Code and accommodated new services, including SMS and MMS.

## What the Code Accomplishes

The Code assists C/CSPs and EMSPs to define processes that help them work with end users, NSRP, ECP, Helplines and law enforcement agencies to address Life Threatening Communications and Unwelcome Communications.

## How the Objectives are Achieved

In the original development of the Code, it was agreed that the best response to a situation involving a Life-Threatening Communication is to inform Police who are in a position to provide a response in conjunction with emergency services. C/CSPs and the NRSP are obliged under this Code to maintain a single point of contact available 24 hours a day 7 days per week. It also requires that procedures be established and maintained to ensure that requests for information or a Communications Trace can be initiated at the request of the Police Communications Centre without undue delay.

C/CSPs and the NRSP continue to maintain policies and procedures for dealing with Unwelcome Communications reported by customers, Suppliers, Helplines and the Emergency Call Service (ECS). The Code rules set out a consistent framework for resolving Unwelcome Communication matters based on the results of communication tracing and the issuing of warning letters to the A-Party Customer of the originating Carriage Service.

## Benefits to Consumers

Consumers benefit from the continued adherence to the principles contained in this Code. In particular, consumers should have confidence that the industry treats the issue and resolution of Unwelcome Communications as a matter of importance. This will be enhanced if all C/CSPs and the NRSP maintain a high level of compliance.

Similarly, consumers have a right to expect that C/CSPs will take all reasonable steps to assist Police in a situation involving a Life-Threatening Communication.

## Benefits to Industry

The Code provides the industry with clearly defined rules for the timely and efficient handling of Life-Threatening Communications and Unwelcome Communications. These rules are based on benchmarks that have already been tried and tested under the previous Code and have been demonstrated to operate effectively.

Importantly the Code does not impose any significant barriers to new entrants to the telecommunications industry. The benefits to the community and telecommunications consumers will outweigh any additional cost to the industry.

## Cost to Industry

Other than the requirement to maintain a 24 hours a day 7 days a week point of contact, the C/CSPs and the NRSP are unlikely to incur any significant cost as a result of

meeting the procedural provisions of the Code. However, there may be additional costs arising from the requirement to, where possible, capture, store and archive Communications Records associated with new types of Carriage Services.

The extent of these costs will depend on the technology employed, the availability of records and whether they are reasonably required for a business purpose other than under this Code.

## 2023 Revision

The 2023 revisions made to the Code include:

- updates to reference documents;
- the addition of clause 1.5 in relation to the handling of personal information;
- a definition for CLI Spoofing being added;
- minor revision to the definition of Pattern of Unwelcome Communications and also Unwelcome Communications for clarity;
- the addition of clause 4.4.14 to clarify information sharing when identifying a pattern of Unwelcome Communications from an offender who has moved Suppliers;
- a reduction in timing before a second warning letter is sent;
- consideration of circumstances for domestic and family violence situations, including a reduction in timings for warning letters and service suspension; and
- updates to warning letter templates in the Appendices.

## 2024 Amendment

The amendment in 2024 is to align with an amendment made *to The Telecommunications Act 1997* which removes the word 'and imminent' from the criteria for consideration by Police when a request to release information is sent from Police Comms Centre staff to a carrier or CSP when Police hold fears for the life or safety of a person.

The Department of Infrastructure, Transport, Regional Development, Communications and the Arts (DITRDCA) has published the Policy Statement of Intent for Section 287 of the Telecommunications Act 1997 on its website which provides guidance on the disclosure of protected information about telecommunications customers, in relation to finding missing persons under section 287 of the Telecommunications Act 1997.

# 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 Section 287 of the Act permits persons to disclose or use personal information of another person if they believe on reasonable grounds that the disclosure or use is reasonably necessary to prevent or lessen a serious threat to the life or health of a person.

1.1.3 The development of the Code has been facilitated by Communications Alliance through a Working Committee comprised of representatives from the telecommunications industry, law enforcement agencies and consumer groups.

1.1.4 Section 474.17 of the *Criminal Code* within the *Criminal Code Act 1995* provides protection for Customers against communications that are menacing, harassing or offensive.

1.1.5 Section 313(1) of the Act imposes a legal obligation on a Carrier or CSP to do the Carrier's best or CSP's best to prevent telecommunications networks and facilities from being used in, or in relation to, the commission of offences against the laws of the Commonwealth or of the States and Territories.

The processes established within this Code enable socially responsible operation and help C/CSPs meet their obligations under section 313(1) of the Act, by reflecting best efforts across the telecommunications industry to prevent Carrier networks from being used in the commission of offences e.g., disconnecting services which are being used to make menacing, harassing or offensive telephone communications.

1.1.6 Section 279 of the Act permits an employee of a C/CSP to disclose information and use information where its use is made in the performance of the person's duties as an employee, such as the duties in section 313(1) of the Act.

1.1.7 The Code should be read in the context of other relevant codes, guidelines and documents including:

C661 – **Reducing Scam Calls and Scam SMs** Industry Code**;** and

G660 **Assisting Customers Experiencing Domestic and Family Violence** Industry Guideline.

*NOTE: Scam communications are out of scope for this Code.*

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

(a) the Act;

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

(c) the *Telecommunications (Interception and Access) Act 1979* (Cth);

(d) *the Telecommunications (Emergency Call Service) Determination 2019;*

(e) the *Criminal Code Act 1995* (Cth);

(f) the *Do Not Call Register Act 2006* (Cth)*;*

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

(h) the *Spam Act 2003* (Cth).

1.1.9 If there is a conflict between the requirements of the Code and any requirements imposed on a Supplier or the NRSP by statute, the Supplier or the NRSP will not be in breach of the Code by complying with the requirements of the statute.

1.1.10 Compliance with this Code does not guarantee compliance with any legislation. The Code is not a substitute for legal advice.

1.1.11 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 registered by the Australian Communications and Media Authority (ACMA) under section 117 of the Act.

## 1.3 Scope

1.3.1 The Code applies to the following sections of the telecommunications industry under section 110 of the Act:

(a) Carriers;

(b) CSPs; and

(c) Electronic Messaging Service Providers (EMSP).

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 as a CSP; or

(c) carrying on business as an EMSP; or

(d) supplying goods or service(s) for use in connection with the supply of a listed Carriage Service.

1.3.3 The Code deals with the following telecommunications activities:

(a) carrying on a business as the NRSP; or

(b) carrying on business as an Emergency Call Person (ECP).

1.3.4 The Code applies only where assistance has been requested in the following situations:

(a) where information is disclosed or used under section 287 of the Act or in anticipation of such a disclosure or use;

(b) where Suppliers or the NRSP are attempting to resolve an Unwelcome or Life-Threatening Communication issue for a B-Party Customer; or

(c) where the ECP or the Helpline are attempting to resolve an Unwelcome or Life-Threatening Communication issue.

*NOTE: This may involve a breach of section 474.17 or 474.18 of the Criminal Code Act 1995.*

1.3.5 The Code does not apply to requests made by law enforcement agencies for information under Chapter 4, Part 4-1, Division 4 of the *Telecommunications (Interception and Access) Act 1979*.

1.3.6 Without limiting a Supplier's obligations under this Code to address Unwelcome Communications, this Code does not create requirements for Suppliers to investigate the origins of an Unwelcome Communication that is:

(a) a SMS or MMS sent from or received by a mobile handset that does not have a Public Number issued by an A-Party Supplier in Australia; or

(b) sent from a non-Public Number operating out of a country other than Australia; or

(c) sent from an email service other than an email service provided by that Supplier; or

(d) sent from a shared public resource, for example a public telephone; or

(e) sent from an Over The Top (OTT) service, other than from an A-Party Supplier in Australia.

*NOTE: Complaints about Unwelcome Communications may also be dealt with under other Australian regulation, including various dispute resolution schemes. For example:*

(a) *complaints about Unwelcome Communications that concern telemarketing may be dealt with under the Do Not Call Register Act 2006 and/or the Privacy Act 1988;*

(b) *complaints about Unwelcome Communications that are unsolicited commercial electronic messages (SMS, MMS, email, etc.) may be dealt with under the Spam Act 2003;*

(c) *the Telecommunications Industry Ombudsman (TIO) may deal with complaints concerning telemarketing on behalf of an Australian C/CSP; and*

(d) *the ASIC/ACCC consumer focused booklet "Dealing with debt collectors: Your rights and responsibilities" may be relevant for complaints that concern collections and debt recovery practices; and.*

(e) *the ASIC/ACCC guideline "Debt collection guideline for collectors & creditors" may be relevant for creditors, collectors and debtors to understand their rights and obligations.*

*C/CSPs are required to ensure that Unwelcome Communications are stopped and to meet their obligations under the Code. The existence of contact limitations for organisations such as those noted in the ASIC/ACCC "Dealing with debt collectors: Your rights and responsibilities" and "Debt collection guideline for collectors & creditors" does not in any way alter the obligations upon C/CSPs.*

## 1.4 Objectives

1.4.1 The objective of the Code is to provide a standard procedure for the cooperative handling, including Communication Tracing, by Suppliers and the NRSP of communications which:

(a) traverse the network(s) of one or more Suppliers; and

(b) are connected with Life Threatening Communications or a Pattern of Unwelcome Communications.

1.4.2 The objectives of each section are detailed in that section.

## 1.5 Privacy obligation

1.5.1 Suppliers must handle personal information relating to Unwelcome Communications in accordance with the Australian Privacy Principles in the Privacy Act.

*NOTE: Part 13 of the Act and the Australian Privacy Principles contained in the Privacy Act 1988 (Cth) require that personal information collected by C/CSPs is only used and disclosed for purposes for which it was collected. The Code ensures that any information about the person making the communication or the person receiving the communication in relation to Life Threatening Communications or Unwelcome Communications remains with that party's Carrier or Carriage Service Provider, and is not further disclosed, except:*

- *where the Supplier believes on reasonable grounds that such disclosure or use is reasonably necessary to prevent or lessen a serious threat to the life or health of a person; or*

- *where such a disclosure is required in the course of the investigation by Police of Life-Threatening Communications; or*

- *where the B-Party Supplier, after receiving the consent of their Customer, must disclose information to the A-Party Supplier in the context of handling Unwelcome Communications; or*

- *where such disclosure is required in the course of the investigations of the Emergency Call Service.*

*Australian Privacy Principle 13 requires that either upon request of a Customer, or where a C/CSP is satisfied that personal information about an individual is inaccurate, out of date, incomplete, irrelevant or misleading it must take steps that are reasonable in the circumstances to correct that personal information. This applies to personal information collected under this Code, including clauses 3.1.6, 4.4.5, 4.4.6 and 4.4.25.*

## 1.6 Code review

The Code will be reviewed every 5 years, or earlier in the event of significant developments that impact on the Code or a section within the Code.

## 1.7 Powers of the Telecommunications Industry Ombudsman to handle complaints under the Code

Under section 114 of the Act and subject to the consent of the TIO, the Code confers on the TIO the functions and powers of:

(a) receiving;

(b) investigating;

(c) facilitating the resolution of;

(d) making determinations in relation to;

(e) giving directions in relation to; and

(f) reporting on

complaints made by the end users of a Carriage Service about matters arising under or in relation to the Code, including compliance with the Code by those industry participants to whom the Code applies.

# 2 ACRONYMS, DEFINITIONS AND INTERPRETATIONS

## 2.1 Acronyms

For the purposes of the Code:

**ACMA**

means Australian Communications and Media Authority

**AMTA**

means Australian Mobile Telecommunications Association

**C/CSP**

means Carrier/Carriage Service Provider

**CCS**

means Common Channel Signalling

**CIC**

means Circuit Identification Code

**CLI**

means Calling Line Identity

**CSI**

means Communications Service Identification

**CSP**

means Carriage Service Provider

**CTCC**

means Call Trace Coordination Centre

**DoS**

means Denial of Service

**ECP**

means Emergency Call Person

**ECS**

means Emergency Call Service

**EMSP**

means Electronic Messaging Service Provider

**ESO**

means Emergency Service Organisation

**IMEI**

means International Mobile Equipment Identifier

**ISP**

means Internet Service Provider

**MMS**

means Multimedia Message Service

**MSN**

means Mobile Service Number

**NRS**

means National Relay Service

**NRSP**

means National Relay Service Provider

**OTT**

means Over The Top service

**PCC**

means Police Communication Centre

**PMTS**

Public Mobile Telecommunications Service

**PSTN**

means Public Switched Telephone Network

**SMS**

means Short Message Service.

**STS**

means Standard Telephone Service

## 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.

***A-Party Supplier***

means the Supplier of the A-Party Carriage Service for that communication. In cases of termination of inbound international Unwelcome Communications this means the Supplier who provides the Dummy CSI in lieu of the full international E.164 number in accordance with ACIF G500:2000.

***Australia***

has the meaning given by section 7 of the Act.

***Australian Privacy Principles***

has the meaning given by section 6 of the *Privacy Act*.

***B-Party***

means the individual or entity receiving the communication.

***B-Party Supplier***

means the Supplier of the B-Party Carriage Service for that 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.

***Call Trace Coordination Centre***

means the C/CSP's centre that coordinates the tracing of communications that traverse that C/CSP's network(s).

***Carriage Service***

has the meaning given by section 7 of the Act.

*NOTE: For the purposes of this Code a Carriage Service may include any form of communication, including, but not limited to:*

(a) *voice telephony*

(b) *video telephony*

(c) *messaging service(s) (e.g., SMS, MMS, etc.)*

(d) *email*

(e) *communications via the National Relay Service*

*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 a scenario where a false CLI has been injected into the A-Party communication.

***Communications Record***

means communications setup information identifying the A-Party, the B-Party, date, time and duration of the communication. Depending on the communications technology employed, this information may or may not be:

(a) reasonably required for business reasons;

(b) readily available; or;

(c) reasonable to capture, store and retain.

*NOTE: For example, Communications Records for STS (including public mobile calls) are collected and retained by C/CSPs for billing and data retention purposes. While records of SMS messages sent by an A-Party may be retained by the A-Party Supplier, they may not be readily available for SMS messages originating from all Suppliers' networks.*

***Communications Service Identification***

means information extracted from a telecommunications network that indicates the identity of the A-Party Carriage Service from which the communication was initiated.

*NOTES:*

*1. For the purposes of this Code, the CSI may include, but is not limited to:*

(a) *a telephone number;*

(b) *an email address; or*

(c) *an IP address.*

*2. A CSI can be modified or masked and may not reflect the true point of origin of the communication. CSPs may need to be mindful of ensuring they confirm the bona fides of the CSI.*

***Communications Trace***

means the tracking of a communication in progress to identify the A-Party and the B-Party and, in the context of this Code, relating to communications that traverse points of interconnection between two or more Carrier networks.

***Customer***

means the person, or that person's authorised agent, who is contracted with the Supplier for the supply of a Carriage Service.

> *NOTE: For the purposes of this Code, Customer includes the end user of that Carriage Service only when that person is the party receiving, making or reporting a Life Threatening or Unwelcome Communication.*

***Denial of Service***

means a deliberate or inadvertent attempt to make access to the ECP or a Helpline unavailable to its intended users.

***Disconnected***

means that the Carriage Service to which the CSI is associated has been cancelled, either at the request of the Customer, or as a result of CSP action e.g., the culmination of ongoing Unwelcome Communications.

> *NOTE: Once a Carriage Service has been Disconnected, the Carriage Service to which the CSI is associated cannot be used to send or receive any communications except to the Emergency Service Numbers 000 and 112 in the case of a mobile telephone service.*

***Domestic and Family Violence***

has the meaning given by the G660 **Assisting Customers Experiencing Domestic and Family Violence** industry guideline.

***Dummy CSI***

means the CSI which is "data filled" as the A-Party Carriage Service identification for specific traffic cases in order to indicate to the receiving Carrier network the origin of the communication. This is required where technology or inter-Carrier agreements do not allow the delivery of the actual or true CSI of the A-Party who initiated the communication.

***Electronic Messaging Service Provider***

has the meaning given by section 108A of the Act.

***Emergency Call Person***

has the meaning given by section 7 of the Act.

> *NOTE: The ECP answers calls to 000 or 112, and the NSRP answers calls to 106.*

***Emergency Call Service***

has the meaning given by section 7 of the Act.

***Emergency Service Number***

has the meaning given by the Telecommunications Numbering Plan 2015.

***Emergency Service Organisation***

Has the meaning given by section 147 of the *Telecommunications (Consumer Protection and Service Standard) Act 1999*.

| |
|---|
| *NOTE: This includes a police force or service, a fire service or an ambulance service.* |

***Helpline***

means an organisation that uses a Carriage Service to provide listening, emotional support and/or advice to anyone in emotional distress, in an individual, family or psycho-social crisis, who is asking for support, and could be feeling lonely, isolated, unhappy, frightened, worried, in shock or suicidal.

| |
|---|
| *NOTE: To access the processes set out in section 5 of this Code, Helplines are required to complete the Helpline Application Form and be registered on the Helpline register maintained by Communications Alliance.* |

***Life Threatening Communication***

means a communication in relation to which a person believes on reasonable grounds, that action is required to prevent or lessen a serious threat to the life or health of a person.

| |
|---|
| *NOTE: A Life-Threatening Communication is one which gives a person reasonable grounds to believe that there is a serious threat to the life or health of a person and may include, but is not limited to an event such as:*<br><br>(a) *a person being seriously injured;*<br><br>(b) *a bomb threat*<br><br>(c) *an extortion demand;*<br><br>(d) *a kidnapping; or*<br><br>(e) *a threat to public safety.* |

***Local Access***

means direct network connection of a Carriage Service through the Australian telecommunications network through which the A-Party originates or the B-Party receives that particular communication.

***National Relay Service***

means a service designed to provide access to a STS to people who are deaf or have a hearing or speech impairment. The NRS is described in section 5 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999 (Cth)*.

***National Relay Service Provider***

means the organisation with the responsibility of providing the NRS.

*NOTE: Further information on the NRS can be found on the NRS website at: http://relayservice.gov.au/.*

***Over The Top service***

an Over-The-Top (OTT) communication application or service is any application or service that provides a communication product over the Internet that:

(a) is operated independently of the underlying Internet access service of an ISP;

(b) overlaps or bypasses traditional telephony or electronic messaging services provided by C/CSPs and EMSPs and their associated billing models.

*NOTE: An example is Skype which can replace a long-distance telephony service provider. This means that an access network provider for data and/or voice services may not have any records of customer communications using OTT communication applications or services.*

***Pattern of Unwelcome Communications***

means Unwelcome Communications that:

(a) are made regularly;

(b) occur ten or more times in a 24-hour period;

(c) occur three or more times over a period of more than 24 hours and less than 120 hours; or

(d) a Customer has brought to the attention of the B-Party Supplier, and which the B-Party Supplier and the A-Party Supplier agree, have been made regularly,

and have been confirmed by the Supplier's Communications Records.

*NOTES:*

1. *A Pattern of Unwelcome Communications does not apply to Unwelcome Communications to the ECS or to Helplines.*
2. *The time period for a Pattern of Unwelcome Communications commences at the first Unwelcome Communication.*
3. *A Pattern of Unwelcome Communications could occur at consistent and/ or regular intervals (for example, made at 2am every Wednesday) with the intent to harass over an extended period.*

***Police Communication Centre***

means the nominated point of contact within the Police, in each State and Territory, which coordinates action between C/CSP(s) and Police in situations involving Life Threatening Communications.

***Public Mobile Telecommunications Service***

has the meaning given by section 32 of the Act.

***Public Number***

has the meaning given by the *Telecommunications Numbering Plan 2015*.

***Specified Number of Unwelcome Communications***

means the number of Unwelcome Communications received, as a threshold agreed between Helplines and Suppliers from time to time, that demonstrates the degree of impact to the Helpline.

*NOTE: The threshold number of Unwelcome Communications may vary from time to time and will be included in the Industry Guidance Note IGN011.*

***Standard Telephone Service***

has the meaning given by section 6 of the *Telecommunications (Consumer Protection and Service Standards) Act 1999*.

***Supplier***

means the C/CSP or EMSP that provides the Carriage Service to the Customer.

***Suspended***

means the state of a Carriage Service to which the CSI is associated that is restricted for a period of time as a result of Customer or CSP action (e.g., following repeated Unwelcome Communications).

*NOTE: During the period of Suspension, the Carriage Service to which the CSI is associated cannot be used to send or receive any communications except to:*

(a) *the Emergency Service Numbers 000 and 112 in the case of a mobile telephone service; and*

(b) *the CSP's Customer contact numbers.*

***Unwelcome Communication***

means use of one or more Carriage Service(s) by an A-Party in a manner which a B-Party (which may include a Helpline, Emergency Call Person or an Emergency Service Organisation) advises or considers is unwelcome, but which is not currently a Life-Threatening Communication.

NOTES: 1. An Unwelcome Communication may also constitute a criminal offence under the *Criminal Code Act 1995*. Under section 474.17 of the *Criminal Code Act 1995*, it is a criminal offence if the communication is made in such a way (whether by the method of use of the Carriage Service, the content of the communication, or both) that a reasonable person would regard it as being, in all the circumstances, menacing, harassing or offensive.

2. Under section 474.18 of the *Criminal Code Act 1995*, it is a criminal offence if the communication is made to the ECS: with the intention of inducing a false belief that an emergency exists; or is made for a purpose otherwise than reporting an emergency and is vexatious.

*3. For example, an Unwelcome Communication could be a repeated communication from an incorrectly programmed fax service or message bank service.*
*4. The definition of Unwelcome Communication includes:*
*(i) communications to a B-Party by the A-Party using one or more forms of Carriage Service e.g., Unwelcome Communications could include calls made from more than one Public Number used by the A-Party to one or more Carriage Services used by the B-Party;*
*(ii) communications to the B-Party via one or more of the same type of Carriage Service used by the same B-Party e.g., Unwelcome Communications could include calls made to more than one Public Number used by that B-Party from a single source;*
*(iii) use of a Carriage Service to make a call to the ECS that is non-genuine, malicious, vexatious or obscene; and improper use of the ECS.*

***Zero Rated Communications***

means communications which are answered but not charged to the A-Party.

## 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 include 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, officer, employee, volunteer, agent and/or subcontractor (including but not limited to, persons taking by novation) and assigns.

# 3 HANDLING OF LIFE-THREATENING COMMUNICATIONS

## Summary

*This section requires Suppliers to:*

- *respond to all requests for assistance with Life Threatening Communications without unreasonable delay; and*
- *provide the details requested by Police in relation to Life Threatening Communications.*

## Objectives

*The objectives of this section are to:*

- *set out the processes for a Supplier to handle Life Threatening Communications; and*
- *set out methods for a Supplier to handle other communications that might raise concern for a person's life or personal safety.*

## 3.1 General

*NOTES:*

1. *A Life-Threatening Communication may require immediate Communications Trace action to prevent or lessen the threat to life or health.*

2. *Life-Threatening Communications demand immediate, predictable and coordinated action on the part of all Suppliers and the NRSP involved to ensure the Communications Trace has the best chance of success.*

3. *To improve efficiency and response times the PCC should make their request for a Communications Trace to the Call Trace Coordination Centre (CTCC) which they judge to be appropriate. See Appendix A for a flow chart of the process.*

4. *Police should make their requests for information relating to Life Threatening Communications by hard copy transmitted by fax or other agreed means. This should be accompanied by a telephone call.*

5. *A Supplier may initiate a Communications Trace for a Life-Threatening Communication, for example in a medical emergency call from the A-Party. In such a case, the Supplier must inform the appropriate PCC. If a person other than the A-Party expresses concern for a person's life or personal safety that person should engage the appropriate ESO. If the customer service representative is talking to the A-Party directly and during that conversation the customer service representative believes on reasonable grounds that a person has a serious threat against his or her life or health, the customer service*

*representative should engage the Police via a telephone call to 000 and release all information known about the person that would be needed by Police to dispatch emergency resources to meet that situation involving a Life Threatening Communication.*

*6. Suppliers and the NRSP should ensure that the access, use and disclosure of information are in accordance with Part 13 of the Act, the Australian Privacy Principles and the Privacy Act. This includes ensuring the security and confidentiality of the information.*

*7. Where a service is not covered by the Code, the customer should seek to identify the service and contact the service supplier directly.*

*8. Suppliers may not be able to take action in the following scenario when investigating a Life-Threatening complaint in any situation where the A Party Customer cannot be identified. e.g., where a person may be using CLI Spoofing of a number (see IGN010).*

3.1.1 Suppliers and the NRSP must only release information to the PCC and the requesting CTCC in relation to Life Threatening Communications:

(a) under section 287 of the Act; and

(b) in accordance with the Australian Privacy Principles in the *Privacy Act*.

3.1.2 Suppliers must encourage the originators of requests for Communications Traces in a situation involving a Life-Threatening Communication to make them through the PCC.

3.1.3 Suppliers and the NRSP must respond to all requests for assistance in relation to Life Threatening Communications without unreasonable delay.

3.1.4 Where Suppliers and the NRSP become aware of a situation involving a Life-Threatening Communication they must tell the person to call the Police directly, and also report the facts to the appropriate PCC via the 000 ECS or the 106 text ECS.

3.1.5 If a person in contact with the NRSP asks a staff member directly (i.e., not in the content of a relayed call) for assistance in a situation involving a Life-Threatening Communication, then the NRSP must advise the person to contact the Police. If the NRSP believes on reasonable grounds that a person faces a serious threat to his/her life or health, the NRSP must also report the facts, including the CSI, if it is available, to the appropriate PCC via the 000 ECS or the 106 text ECS.

3.1.6 To effectively manage Life Threatening Communications for Customers, it is recommended that Suppliers retain, where practicable:

(a) Communications Records of communications made or received by the Customer subject to the Life-Threatening

Communication for a period of at least 30 days following the initial contact made by the Customer; and

(b) records of communications with that Customer relating to their Life-Threatening Communications for a period of at least three years, or until the Carriage Service is Disconnected.

## 3.2 CTCC Processes for Life Threatening Communications

3.2.1 As soon as the B-Party CTCC is made aware of the requirement to trace a communication, it must commence the Communications Trace and, if it is necessary to involve another CTCC, must provide the other CTCC with the:

(a) Interconnect Request For Communications Trace form (refer to Appendix C); and

(b) PCC's request via a format similar to that in Appendix B.

3.2.2 As soon as the B-Party CTCC is made aware that tracing of a communication while in progress is required and it is necessary to involve another CTCC, the initiating CTCC must:

(a) issue the Communications Trace request orally to the other CTCC;

(b) provide the other CTCC with the Interconnect Request For Communication Trace form (refer to Appendix C); and

(c) provide the other CTCC with the PCC's request via a format similar to that in Appendix B.

3.2.3 When an oral request for a Communications Trace is received, the Supplier or NRSP must collect the required information.

3.2.4 Subject to 3.2.3, a CTCC:

(a) must not release information, until the written request is received, if the CTCC is unsure of the origin of the request;

(b) may release information where the origin of the request is known and authorised to receive that information.

3.2.5 Any CTCC receiving the Communications Trace request must:

(a) arrange for an immediate Communications Trace if the communication is still in progress; or

(b) arrange to have the Communications Records queried if the call is no longer in progress.

3.2.6 CTCCs must make their requests for information relating to Life Threatening Communications by hard copy transmitted by fax or other agreed means which can be evidenced. This should be accompanied by a telephone call.

3.2.7 The CTCC that determines the identity of the A-Party must return the Communications Trace results by telephone and fax to the PCC immediately when they are available, subject to receipt of the appropriate written request in accordance with clause 3.2.34 if the CTCC is unsure of the origin of the request.

3.2.8 In certain circumstances, it may be necessary to implement a Communications Trace on a Carriage Service if the Supplier has such a facility. The PCC should request the appropriate Carrier to trace a communication using the PCC Request Form (refer to Appendix B). Any Carrier receiving a request for another Carrier must pass it to the correct Carrier.

*NOTE: The management of Life-Threatening Communications can be greatly simplified using Communications Trace technology and Suppliers are encouraged to provide this facility on their networks.*

3.2.9 When responding to a request for information initiated by the Police in regards to a Life-Threatening Communication, the Supplier CTCC must provide the details requested by the Police. In addition, if the Life-Threatening Communication was made from a PMTS, then the A-Party CTCC and/or the B-Party CTCC must provide the cell location information if requested.

3.2.10 Where the NRSP has facilitated the A-Party call to the B-Party the CTCC of the B-Party must engage the NRSP to determine the actual A-Party.

*NOTES:*
*1. Figure 4 in Appendix D is a flowchart on the management of Unwelcome Communications involving the NRSP. A similar process should apply to the management of Life-Threatening Communications involving the NRSP.*

*2. In resolving some Life-Threatening Communications situations, it may be necessary to Suspend a Carriage Service to avoid a Supplier being in breach of section 313(1) of the Act.*

# 4 HANDLING OF UNWELCOME COMMUNICATIONS

## Summary

*This section requires Suppliers to:*

- *identify the A-Party where there is a Pattern of Unwelcome Communications; and*
- *perform a range of actions to prevent further Unwelcome Communications.*

## Objectives

*The objectives of this section are to:*

- *set out the processes for a Supplier to handle a Pattern of Unwelcome Communications; and*
- *set out obligations for Suppliers to communicate information to Customers.*

## 4.1 General

*NOTES:*

*1. Unwelcome Communications relate to communications that are considered by the recipient of the communication to be unwelcome. They do not normally require time critical responses (other than when they impact on the ECS, ESOs or Helplines which do require a time critical response) and do not necessarily involve the Police. See Appendix D for flow charts of the processes for handling Unwelcome Communications.*

*2. Where a service is not covered by the Code, the Customer should seek to identify the service and contact the service Supplier directly.*

4.1.1 When engaged in an Unwelcome Communication investigation, Suppliers must take all reasonable steps to ensure effective communications between the Suppliers involved and work cooperatively to investigate and resolve the Unwelcome Communication.

*NOTE: Suppliers should not act as middlemen or as a clearing house for matters that do not directly involve them.*

4.1.2 The B-Party Supplier dealing with the Unwelcome Communications must ensure that the Unwelcome Communications complaint:

(a) has come from their Customer;

(b) relates to a Pattern of Unwelcome Communications;

(c) includes at least one Unwelcome Communication that was received in the past 30 days and

(d) is acknowledged within 1 Business Day of receipt.

4.1.3 If a B-Party Suppliers Customer believes that the Unwelcome Communications are as a result of a Domestic and Family Violence situation, a B-Party Supplier must take this information into consideration when informing their action as per clause 4.4.18.

4.1.4 If the details identified in clause 4.1.3 include sensitive information about the B-Party Customer or others as defined in the Privacy Act, the B-Party Supplier must obtain the B-Party Customer's consent to disclose the details to the A-Party Supplier.

*NOTE: Refer to G660 Assisting Customers Experiencing Domestic and Family Violence for assistance in these considerations.*

4.1.5 To effectively manage Unwelcome Communications for Customers, it is recommended that Suppliers retain, where practicable:

(a) Communications Records of communications made or received by the Customer subject to the Unwelcome Communication for a period of at least 30 days following the initial contact made by the Customer; and

(b) records of all other communications with that Customer relating to their Unwelcome Communications for a period of at least three years after the last communication with the Customer.

4.1.6 Where the Supplier has had no referrals of Unwelcome Communications relating to the CSI of the A-Party Customer for the previous three years, the warning letter process for an A-Party Customer must begin again in the event there are further Unwelcome Communications. The matter will be treated as a new case with no precedents to be taken into account irrespective of the stage at which a prior process had reached.

4.1.7 In the event there were Unwelcome Communications within the previous three years from an A-Party Customer to the same person, the process for an A-Party Customer must be treated as continuation of the previous case and will continue from the stage at which a prior process had reached.

## 4.2 Communication with Customers

4.2.1 Communication with a Customer must only be conducted by their Supplier.

*NOTE: For example, the Supplier is, in the case of:*

(a) *CSP reselling Local Access calls, that CSP;*

(b) *PMTS, the CSP that provides that Carriage Service;*

(c) *an email service, the EMSP that provides that email service.*

4.2.2 B-Party Suppliers must inform their Customers that the Customer may report Unwelcome Communications to the Police at any time.

4.2.3 The B-Party Supplier must try to resolve an Unwelcome Communications issue before referring their Customer to the Police, even though their Customer may report the matter to the Police at any time.

*NOTE: B-Party Suppliers would normally refer their Customer to the Police when their Customer perceives the communications to be particularly threatening or offensive and their Customer is not prepared to wait the required time period for the matter to be resolved through a warning letter process.*

4.2.4 The B-Party Supplier must suggest to their Customer the options they have available. Some possible options may include, but are not limited to the following:

(a) terminate communication with the A-Party initiating the communication immediately;

(b) use an answering machine or voicemail to screen callers;

(c) use calling number display facilities to screen calls and choose which calls to answer;

(d) if Unwelcome Communications are from a fax machine, divert the calls to a fax machine to assist in identifying the calling fax;

(e) do not send SMS or MMS to a B-Party who they do not wish to see their CSI;

(f) where they have a separate EMSP, consult that EMSP on how to block or filter email identified from a particular source;

(g) change their contact Public Number(s) and/or email address(es) and not make their new contact details publicly available, for example by having the new Public Number unlisted in public number directories; or

(h) contact the Police.

*NOTE: The B-Party Supplier should advise their Customer that each EMSP should have an abuse@xxxxxxx.xx email address to which they can report all unwelcome emails. The B-Party Supplier should assist their Customer in extracting information from the unwelcome email to identify the A-Party Supplier to enable the B-Party Customer to contact that EMSP.*

4.2.5 If the Customer indicates to its B-Party Supplier that either they do not want to proceed with the options in clause 4.2.4, or in addition to these options, they want the matter investigated, the B-Party Supplier must:

(a) advise their Customer that the investigation and possible sending of warning letter(s) by the A-Party Supplier requires disclosure of the CSI of their Customer's service to the A-Party Supplier and the recipient of the warning letter(s);

(b) confirm that their Customer consents to this disclosure of the CSI of their Customer's service;

(c) advise their Customer not to delete the Unwelcome Communication(s) and;

(d) request that their Customer make detailed records of the received Unwelcome Communications including:

(i) the origin of the communication;

(ii) the date;

(iii) the time; and

(iv) the approximate duration

of the Unwelcome Communications.

*NOTE: The B-Party Supplier may also explain to their Customer that disclosure of the CSI of their Customer's service in warning letter(s) can enable the recipient of the warning letter(s) to determine which communications from the relevant service were unwelcome so the recipient can take steps to prevent future Unwelcome Communications.*

4.2.6 If the Customer indicates to its B-Party Supplier that they do not consent to the disclosure of their CSI of their service receiving the Unwelcome Communications to the recipient of the warning letter, then the B-Party Supplier must inform their Customer that no further action can be taken under this Code.

4.2.7 Where, subject to clause 4.2.5, an A-Party Supplier has commenced the investigation and warning letter process the A-Party Supplier must, in a timely manner:

(a) advise the B-Party Supplier of the outcome of that process;

(b) provide a reason to the B-Party Supplier who originated the request for any inability to send a warning letter; and

(c) where the B-Party Supplier has determined a Pattern of Unwelcome Communications that involves multiple A-Party services that may have been provided by multiple A-Party Suppliers and requested the sending of a warning letter, the A-Party Suppliers must rely on the B-Party Supplier's

Communications Records as sufficient evidence to confirm a Pattern of Unwelcome Communications.

*NOTE: Suppliers may not be able to take action in the following scenarios when investigating an Unwelcome Communication complaint:*

*(a) when a person, making Unwelcome Communications moves from one A-Party Supplier to another;*

*(b) when a person uses multiple communications services associated with one or multiple A-Party Suppliers to make Unwelcome Communications;*

*(c) when a person makes Unwelcome Communications from international origins that are associated with an Australian entity or Public Number e.g., from offshore call centres or a global roaming mobile telephone associated with a Public Number;*

*(d) when a person makes Unwelcome Communications from a communications service for which the A-Party Supplier is unable to identify the source of the communication, e.g., one way VoIP out service(s); and*

*(e) in any situation where the A Party Customer cannot be identified. e.g., where a person may be using CLI Spoofing of a number (see IGN010).*

4.2.8 Where an A-Party Supplier needs to communicate with its Customer, including where it considers that communicating a warning to its Customer by physical "warning letter" under this Code may not be successful, for example where an address is not available, or where the address may not be reliable or up-to-date, then the A-Party Supplier may communicate by its usual method of communication with the Customer or by one or more other means, whichever is likely to be most effective, including (but not limited to):

(a) email;

(b) SMS;

(c) MMS; or

(d) voice call.

4.2.9 If an A-Party Supplier communicates a warning by one or more other means under clause 4.2.8:

(a) this communication may be in addition to, or in substitution for (for example where an address is not available), a physical warning letter;

(b) this communication will satisfy the requirements to send a warning letter where it is referred to in this Code; and

(c) the A-Party Supplier should use best efforts to establish and record proof of delivery and / or receipt by the A-Party Customer.

4.2.10 An inability on the part of the A-Party Supplier to establish proof of delivery and / or receipt of a warning letter is not grounds to delay or discontinue any process set out in this Code.

## 4.3 Identification of a CSI

4.3.1 If a Pattern of Unwelcome Communications is identified, then the B-Party Supplier must attempt to identify the A-Party. This may be achieved by examination of Communications Records or the implementation of Communication Trace facilities on the Carriage Service.

4.3.2 A Supplier must use Communications Records relating to unanswered or Zero-Rated Communications, if available, to establish a Pattern of Unwelcome Communications.

4.3.3 Where automatic Communication Trace facilities are not available for that Carriage Service, the B-Party Supplier must make arrangements with other Suppliers to undertake Communication Tracing using any appropriate Communications Records.

*NOTE: The management of Unwelcome Communications can be greatly simplified using Communications Trace technology and Suppliers are encouraged to provide this facility on their networks.*

4.3.4 If a Supplier receives a formal advice from Police stating that assistance would be appreciated to support an investigation of an Unwelcome Communication complaint under section 474.17 of the *Criminal Code Act 1995* then the Supplier must provide the requested information to Police.

*NOTE: A formal advice from Police that might satisfy this clause could be in a format similar to the example in Appendix E.*

4.3.5 Where the NRSP is identified by its Carrier as being the A-Party of an Unwelcome Communication complaint, the NRSP must inspect its Communications Record to determine if there is a Pattern of Unwelcome Communications.

4.3.6 If the NRSP:

(a) identifies a Pattern of Unwelcome Communications; and

(b) receives an Unwelcome Communication action request in a format similar to that in Appendix F;

then the NRSP must as soon as practicable, and within 10 Business Days, provide to its Carrier only the CSI of the A-Party.

4.3.7 A Supplier must take all reasonable steps to be satisfied that they have identified the CSI of the alleged Unwelcome Communications.

## 4.4 Processes in Response to a Pattern of Unwelcome Communications

4.4.1 If the B-Party Supplier identifies the A-Party from the CSI and the A-Party is:

(a) a Customer of the B-Party Supplier, then the B-Party Supplier must send an initial warning letter to the Customer within two Business Days and the B-Party Supplier must treat that letter as if it is an initial warning letter to the B-Party Supplier.

(b) a Customer of a Supplier that is a different party from the B-Party Supplier, then the B-Party Supplier must send an Unwelcome Communication action request to the A-Party Supplier within two Business Days and the A-Party Supplier must treat that request as if it is an initial warning letter.

(c) the same party as the B-Party Supplier, then the B-Party Supplier must treat the notice of Unwelcome Communications from the Customer as if it is an initial warning letter to the B-Party Supplier.

4.4.2 An initial warning letter must clearly identify that it is an initial warning letter.

4.4.3 An initial warning letter must include:

(a) the CSI of the B-Party Customer;

(b) the times and dates of the Unwelcome Communications;

(c) the CSI of the A-Party Customer; and

(d) the name and contact details of the A-Party Supplier for further communications.

*NOTES:*

*1. In the case of a simple notification e.g., an A-Party Customer calling one, or few Public Numbers, the format should be similar to the example in Appendix G1. Where the A-Party Customer uses a technology that automates outbound calls the A-Party Supplier may communicate the first warning, including details of the Unwelcome Communications to the A-Party Customer in the manner in which the A-Party Supplier normally communicates with the Customer or via an agreed communication medium where an A-Party Customer has a specific communication need. These forms of communication for the purposes of the requirements of the Code, will be treated as a formal warning consistent with the issuing of an initial warning letter.*

*2. As per clause 4.2.8 it is for the A-Party Supplier to determine the most suitable method for contacting an A-Party Customer to ensure they receive the initial warning letter.*

4.4.4 When a B-Party Supplier requests an action from another Supplier or the NRSP in response to an Unwelcome Communications matter, the B-Party Supplier must provide:

(a) the CSI of the B-Party Customer;

(b) the times and dates of the Unwelcome Communications; and

(c) the CSI of the A-Party Customer.

*NOTE: An action request that might satisfy this clause could be in a format similar to the example in Appendix F.*

4.4.5 After receiving an Unwelcome Communication action request an A-Party Supplier must:

(a) send an acknowledgement of receipt of the Unwelcome Communication action request to the B-Party Supplier within one Business Day;

(b) inspect its Communications Records to determine the validity of the complaint; and

(c) where valid, identify all the circumstances related to the Unwelcome Communication and any extenuating circumstances (also see NOTE under clause 4.4.25).

*NOTES:*

*1. Where the Unwelcome Communication action request has been sent by the B-Party Supplier to the A-Party Supplier via email, the A-Party Supplier should provide an auto email acknowledgement response within one Business Day.*

*2. The Customer is always responsible for the use of the service; however extenuating circumstances may exist that require a more considered approach in dealing with the Unwelcome Communication complaint (also see NOTE under clause 4.4.25).*

4.4.6 If an A-Party Supplier verifies:

(a) there has been a Pattern of Unwelcome Communications after receiving an Unwelcome Communication action request from a B-Party Supplier; and

(b) there are no extenuating circumstances or other matters that caused the Unwelcome Communications as set out in clause 4.4.25,

then the A-Party Supplier must issue an initial warning letter to the Customer of that A-Party CSI within two Business Days.

4.4.7 An A-Party Supplier must complete the requirements of clauses 4.4.5 and 4.4.6 and respond to the B-Party Supplier advising the outcome of its investigations, including whether a Pattern of Unwelcome Communications has been verified and, if so, any extenuating circumstances or other matters that exist and the action, if any, that has been taken:

(a) as soon as practicable; and

(b) within 10 Business Days of the issue of the request by the B-Party Supplier.

*NOTE: In the above clauses 4.4.5 and 4.4.7 the timeframes stated apply to all parties involved within the chain of communication response.*

4.4.8 If the A-Party CSI is not unique to a single Carriage Service (e.g., a VoIP out service), then the A-Party Supplier must inspect its Communications Records to determine the identity of the initiator of the Unwelcome Communication and send an initial warning letter to that party.

4.4.9 If the A-Party Supplier cannot identify a Customer of the A-Party Supplier as the initiator of the Pattern of Unwelcome Communications, then the A-Party Supplier must advise the B-Party Supplier of the fact that the initiator of the Pattern of Unwelcome Communications cannot be identified.

4.4.10 If clause 4.4.9 above applies, then the B-Party Supplier should then advise its Customer that:

(a) the initiator of the Pattern of Unwelcome Communications cannot be identified;

(b) there is no further action that can be undertaken under this Code; and

(c) the Customer may seek assistance from the Police for resolving this issue.

4.4.11 If the A-Party Supplier has acknowledged there are:

(a) Communications Records that provide insufficient information to confirm a Pattern of Unwelcome Communications; and

(b) B-Party Supplier Communications Records that provide sufficient information to confirm a Pattern of Unwelcome Communications,

then the A-Party Supplier must rely on the B-Party Supplier's Communications Records as sufficient evidence to confirm a Pattern of Unwelcome Communications.

4.4.12 If the B-Party Supplier advises the A-Party Supplier that the Pattern of Unwelcome Communications did not cease within 5 Business Days of the A-Party Supplier sending the initial warning letter, then

the A-Party Supplier must, unless subject to clause 4.4.13, send a second warning letter to its Customer.

4.4.13 If the B-Party Supplier advises the A-Party Supplier that the B-Party Customer's complaint relates to a Domestic and Family Violence situation, refer to clause 4.4.18.

4.4.14 Where the B-Party Customer maintains that Unwelcome Communications are still being received from the same "offender" after the A-Party Supplier has issued an initial warning letter and the B-Party Carrier's Communications Records have identified that the Unwelcome Communications are coming from one or more new CSIs for which A-Party Suppliers may not be able to establish a link to the pre-existing Pattern of Unwelcome Communications, then the A-Party Suppliers must:

(a) rely on the B-Party Carrier's Communications Records and the B-Party Supplier's advice that it had established a Pattern of Unwelcome Communications as sufficient evidence to confirm a continuation of a Pattern of Unwelcome Communications, and

(b) issue a second warning letter to the A-Party Customer of the service/s identified in the B-Party Carrier's Communications Records, or suspend/cancel the relevant service, except where it is impractical to do so (e.g. public phone, one-way VoIP service, etc.).

*NOTE: Suppliers may not be able to take action in the following scenarios when investigating an Unwelcome Communication complaint:*

(a) *when a person makes Unwelcome Communications moves from one A-Party Supplier to another;*

(b) *when a person uses multiple communications services associated with one or multiple A-Party Suppliers to make Unwelcome Communications;*

(c) *when a person, makes Unwelcome Communications from international origins that are associated with an Australian entity or Public Number e.g., from offshore call centres or a global roaming mobile telephone associated with a Public Number;*

(d) *when a person makes Unwelcome Communications from a communications service for which the A-Party Supplier is unable to identify the source of the communication, e.g., one way VoIP out service(s); and*

(e) *in any situation where the A Party Customer cannot be identified. e.g., where a person may be using CLI Spoofing of a number (see IGN010).*

4.4.15 A second warning letter must clearly identify that it is a second warning letter.

4.4.16 The second warning letter must include:

(a) the CSI of the B-Party Customer;

(b) the times and dates of the Unwelcome Communications;

(c) the CSI of the A-Party Customer;

(d) notice that it is an offence under section 474.17 of the *Criminal Code Act 1995* to use a Carriage Service in a way that a reasonable person would regard as menacing, harassing or offensive;

(e) a warning that if the Unwelcome Communications continue then the A-Party Supplier will Suspend or Disconnect the Carriage Service associated with the A-Party CSI; and

(f) the name and contact details of the A-Party Supplier for further communications.

*NOTE: In the case of a simple notification e.g., an A-Party Customer calling one, or few Public Numbers, the format should be similar to the example in Appendix H. Where the A-Party Customer uses a technology that automates outbound calls the A-Party Supplier may communicate the second warning, including details of the Unwelcome Communications to the A-Party Customer in the manner in which the A-Party Supplier normally communicates with the Customer or via an agreed communication medium where an A-Party Customer has a specific communication need. These forms of communication, for the purposes of the requirements of the Code, will be treated as a formal warning consistent with the issuing of a second warning letter. Also see Note 2 under Clause 4.4.17.*

4.4.17 If the A-Party Supplier was the source of the Pattern of Unwelcome Communications and the A-Party Supplier is advised by the B-Party Supplier that the Unwelcome Communications did not cease within 5 Business Days of receipt of the initial Unwelcome Communication action request, then the A-Party Supplier must treat the second Communication Action Request as if it was a second warning letter.

*NOTES:*

1. *In respect of the warning letters referred to in 4.4.2 – 4.4.17 above there may be circumstances where a warning letter cannot be sent to the initiator of the Unwelcome Communication e.g. where the A-Party CSI relates to a generic Carriage Service such as a public telephone.*

2. *Where possible the A-Party Supplier should send its warnings via a method that ensures "proof of delivery and / or receipt" to ensure that the A-Party Customer is aware of the complaint and any further action that may result, and to avoid any potential for the A-Party Customer to make a*

*complaint against the A-Party Supplier if/when the Carriage Service is Suspended or Disconnected.*

3. *It is recommended the A-Party Supplier follows up with a telephone call if no response from the A-Party Customer has been received.*

4.4.18 If the B-Party Supplier advises the A-Party Supplier that the Unwelcome Communications have not ceased following receipt by the A-Party Customer of a second warning letter, or in the case of a Domestic and Family Violence situation following the first warning letter, then the A-Party Supplier must Suspend, or if Suspension is not possible, Disconnect, the A-Party Customer's Carriage Service.

*NOTES:*

1. *Not all Carriage Services have the ability to be Suspended - for some this will mean an immediate Disconnection of the Carriage Service.*

2. *The above clause includes where the Customer is the A-Party Supplier.*

3. *The B-Party Customer may also be advised they can contact the Police for further action.*

4. *Refer to Appendix I for a suggested letter for Suspending/Disconnecting a Customer's service.*

4.4.19 If an A-Party Supplier:

(a) Suspended / Disconnected a Carriage Service which has been used to make a Pattern of Unwelcome Communications; and

(b) receives a written undertaking within 10 Business Days from the A-Party Customer of that Suspended / Disconnected Carriage Service that the A-Party Customer will not use any Carriage Service to make further Unwelcome Communications,

then the A-Party Supplier may, at its discretion, offer to restore / reconnect the Carriage Service to the A-Party Customer.

*NOTES:*

1. *Refer to Appendix J for a suggested letter to request restoration/reconnection of a Suspended or Disconnected Carriage Service.*

2. *A digital signature may be used as an acceptable customer acknowledgement in a written undertaking.*

4.4.20 If the A-Party Customer does not provide a written undertaking, as per clause 4.4.19, to the A-Party Supplier that the A-party

Customer will not use the Carriage Service to make Unwelcome Communications in the future, then the A-Party Supplier must immediately Disconnect the Carriage Service(s) used to make the Unwelcome Communications.

4.4.21 If an A-Party Supplier:

(a) Restores / reconnects a Carriage Service that was used to make Unwelcome Communications; and

(b) receives notice of subsequent Unwelcome Communications made from the restored / reconnected Carriage Service within three years of a restoration or reconnection related to a previous Pattern of Unwelcome Communications,

then the A-Party Supplier must immediately Disconnect the Carriage Service(s) used to make the Unwelcome Communications without any further warnings.

*NOTE: Refer to Appendix I for a suggested letter Suspending/Disconnecting a Customer's service.*

4.4.22 If Police request information from a Supplier in connection with an Unwelcome Communications matter, and the information may be held by another Supplier or the NRSP, the Supplier receiving the request must refer the Police to that other Supplier or the NRSP.

4.4.23 A Supplier must not seek Customer information from another Supplier or the NRSP on behalf of the Police.

4.4.24 All Suppliers involved in an Unwelcome Communication complaint must assist the Police in the investigation of that complaint and provide all available information, including:

(a) Communications Records; and

(b) results of Communications Traces.

4.4.25 If, at any point under section 4, after an A-Party Supplier has:

(a) received an Unwelcome Communication action request from a B-Party Supplier;

(b) verified there has been a Pattern of Unwelcome Communications; and

(c) considered all of the circumstances,

and the A-Party Supplier identifies that there are either:

(d) extenuating circumstances that caused the Unwelcome Communications; or

(e) other matters indicating that taking the relevant action would have an unacceptable and/or detrimental impact on the Customer, or others,

the A-Party Supplier may choose to either:

(f) delay taking the relevant action;

(g) not take the relevant action under section 4; or

(h) take another action.

In such cases, the A-Party Supplier must notify the B-Party Supplier and provide details of the relevant extenuating circumstances or other matters; and provide details of the action taken, or relevant action(s) delayed or not taken.

Upon receipt of the notification from the A-Party Supplier, the B-Party Supplier may provide the A-Party Supplier with further information to assist.

*NOTE: Extenuating circumstances may be actions or events that arise which are beyond the Customer's control e.g., the Customer's mobile device was stolen or misplaced, and another party made the Unwelcome Communications.*

*Extenuating circumstances do not excuse an ongoing Pattern of Unwelcome Communications over an extended period of time.*

*Unacceptable and/or detrimental impacts include but are not limited to those where taking an action under section 4 could cause significant harm to the Customer, other people (e.g., the Customer's family members), or the community.*

4.4.26 The B-Party Supplier must keep the B-Party Customer (the recipient of the Unwelcome Communications) informed of progress of the matter and its handling, including whether the A-Party Supplier has proceeded under clauses 4.4.25 (f), (g) or (h).

# 5 UNWELCOME COMMUNICATIONS TO HELPLINES

## Summary

Unwelcome Communications to Helplines may involve, threat, menace, harassment, or cause offence and have the potential to have a higher negative impact to the community than Unwelcome Communications to a single consumer of communications services. Due to the nature of Helpline services, and the need to respond to genuine help seekers, Unwelcome Communications to Helplines require time critical responses by Suppliers to investigate and take action to halt or hinder communications that involve threat, menace, harassment or cause offence.

It is generally recognised that the impact of Unwelcome Communications to Helplines can fall into two categories:

- can cause problems in the ability for genuine users of the services to gain access to help they may need to lessen or prevent injury or loss of life especially where the volume of communications to the Helpline is of concern and could have the effect of potentially emulating a Denial of Service (DoS) attack; and

- can cause psychological trauma to the Helpline call-takers who may be unable to continue to perform their duties and could require counselling.

Unlike calls to 000, calls to Helplines will not deliver to the Helpline network the CSI of a service if that service has been marked as having a restricted Calling Line Identity (CLI) (e.g., private number). The CLI is however carried across the Public Switched Telephone Network (PSTN) Carrier networks and will be available to the B-Party Carrier and therefore to the B-Party Supplier. It would, however, be a breach of the Privacy legislation for the B-Party Supplier to pass the restricted CLI on to the Helpline for the purposes of the Helpline taking action independent of industry or Police.

This section requires Suppliers to:

- *assist Helplines to manage Unwelcome Communications to the Helpline service; and*

- *minimise Unwelcome Communications to Helplines that involve threat, menace, harassment or cause offence.*

## Objectives

The objectives of this section are to:

- *describe the process for the handling of Unwelcome Communications to Helplines; and*

- *describe the process to minimise Unwelcome Communications to Helplines.*

### 5.1 General

5.1.1 The Code relies upon Helplines to co-operate with Suppliers to provide clear information in a timely manner to Suppliers, so they are able to meet their obligations under this Code.

5.1.2 Communications Alliance maintains a register of Helplines, listing the Helplines that are subject to this Code. Suppliers are only subject to the requirements of this Code in relation to Helplines included on the register of Helplines.

5.1.3 A Helpline seeking to access the processes outlined in this Code should contact Communications Alliance and apply to be included on the register of Helplines. Communications Alliance may add or remove Helplines from the register from time to time at its absolute discretion.

5.1.4 The rules in this Code only apply to the extent that Helplines provide all relevant and/or requested information to Suppliers to support actions outlined in this Code.

*NOTE: Helplines should retain all evidence in their possession in connection with any actions undertaken pursuant to this Code, to support law enforcement actions, or for use in future legal or dispute resolution proceedings.*

*Evidence of Unwelcome Communications may include: notes made by a B-Party call recipient, call recordings, chat logs, electronic or hardcopy communications with the A-Party, details of whether the communication involved a threat, menace, harassment or caused offence and any other related records.*

5.1.5 When engaged in an Unwelcome Communication investigation, Suppliers must take all reasonable steps to ensure effective communications between the Suppliers involved and work cooperatively to investigate and resolve the Unwelcome Communication.

## 5.2 Processes in Response to Unwelcome Communications to Helplines

5.2.1 The B-Party Supplier dealing with the Unwelcome Communications to a Helpline must ensure that the Unwelcome Communications complaint:

(a) has come from their Customer;

(b) relates to the Specified Number of Unwelcome Communications;

(c) includes at least one Unwelcome Communication that was received in the past 30 days and

(d) is acknowledged within 1 Business Day of receipt.

5.2.2 If the B-Party Supplier identifies the A-Party from the CSI and the A-Party is:

(a) a Customer of the B-Party Supplier, then the B-Party Supplier must, subject to clause 5.2.16, send an initial warning letter to the Customer within two Business Days and the B-Party

Supplier must treat that letter as if it is an initial warning letter to the B-Party Supplier.

(b) a Customer of a Supplier that is not a different party from the B-Party Supplier, then the B-Party Supplier must send an Unwelcome Communication action request to the A-Party Supplier within two Business Days and the A-Party Supplier must treat that request as if it was an initial warning letter.

(c) the same party as the B-Party Supplier, then the B-Party Supplier must treat the notice of Unwelcome Communications from the Customer as if it is an initial warning letter to the B-Party Supplier.

5.2.3 Subsequent to the notification by the Helpline to the B-Party Supplier about the receipt of the Specified Number of Unwelcome Communications to the Helpline, the B-Party Supplier must notify the A-Party Supplier accordingly to request that the A-Party Supplier:

(a) contact the A-Party Customer to educate the A-Party Customer about the appropriate use of the Helpline; and

(b) inform the A-Party Customer that Unwelcome Communications to the Helpline may constitute a criminal offence.

5.2.4 When a B-Party Supplier requests an action from an A-Party Supplier in response to an Unwelcome Communications matter, the B-Party Supplier must provide:

(a) the CSI of the B-Party Customer;

(b) the times and dates of the Unwelcome Communications; and

(c) the CSI of the A-Party Customer, including where known the IMEI of the mobile device if the A-Party CSI is associated with a PMTS.

*NOTE: An action request that might satisfy this clause could be in a format similar to the example in Appendix F.*

5.2.5 If an A-Party Supplier verifies there has been a Specified Number of Unwelcome Communications after receiving an Unwelcome Communications action request from a B-Party Supplier, then the A-Party Supplier must:

(a) Send an acknowledgement receipt of the Unwelcome Communications action request to the B-Party Supplier within one Business Day of receiving the Unwelcome Communications action request;

(b) issue an initial warning letter to the Customer of that A-Party CSI within two Business Days of receiving the Unwelcome Communications action request to alert the A-Party

Customer that the Carriage Service has been used for Unwelcome Communications and that a criminal offence may have been committed and that the IMEI of the mobile device which was used for Unwelcome Communications may be blocked across all mobile Carriers in Australia; and

(c) respond to the B-Party Supplier within two Business Days of the issue of the request and advise the action that has been taken and provide, where known, the IMEI of the mobile device if the A-Party CSI is associated with a PMTS.

*NOTES:*

1. *Where the Unwelcome Communication action request has been sent by the B-Party Supplier to the A-Party Supplier via email, the A-Party Supplier should provide an auto email acknowledgement response within one Business Day.*

2. *In the case of a simple notification e.g., an A-Party Customer calling one, or a few Public Numbers, the format should be similar to the example in Appendix G2. Where the A-Party Customer uses a technology that automates outbound calls the A-Party Supplier may communicate the first warning, including details of the Unwelcome Communications to the A-Party Customer via an agreed communication medium where an A-Party Customer has a specific communication need. These forms of communication for the purposes of the requirements of the Code, will be treated as a formal warning consistent with the issuing of an initial warning letter. Also see Note 2 under clause 4.4.5.*

3. *It is for the A-Party Supplier to determine if the use of an SMS/MMS or verbal communication may be a suitable method for contacting an A-Party Customer in place of an initial warning letter.*

4. *Suppliers may not be able to take action in the following scenario when investigating an Unwelcome Communication complaint in any situation where the A Party Customer cannot be identified. E.g., where a person may be using CLI Spoofing of a number (see IGN010).*

5. *To identify the IMEI the A-Party Supplier may seek assistance from the A-Party Carrier.*

5.2.6 An initial warning letter must clearly identify that it is an initial warning letter.

5.2.7 An initial warning letter must include:

(a) the CSI of the B-Party Customer;

(b) the times and dates of the Unwelcome Communications;

(c) the CSI of the A-Party Customer; and

(d) the name and contact details of the A-Party Supplier for further communications.

*NOTES:*

1. *The format should be similar to the example in Appendix G2. Where the A-Party Customer uses a technology that automates outbound communications the A-Party Supplier may communicate the first warning, including details of the Unwelcome Communications to the A-Party Customer in the manner in which the Supplier normally communicates with the Customer or via an agreed communication medium where an A-Party Customer has a specific communication need. These forms of communication for the purposes of the requirements of the Code, will be treated as a formal warning consistent with the issuing of an initial warning.*

2. *It is recommended the A-Party Supplier follows up with a telephone call if no response from the A-Party Customer has been received.*

5.2.8 If the A-Party Supplier has acknowledged there are:

(a) Communications Records that provide insufficient information to confirm a Specified Number of Unwelcome Communications; and

(b) B-Party Supplier Communications Records that provide sufficient information to confirm a Specified Number of Unwelcome Communications,

then the A-Party Supplier must rely on the B-Party Supplier's Communications Records as sufficient evidence to confirm a Specified Number of Unwelcome Communications.

5.2.9 If the B-Party Supplier advises the A-Party Supplier that the Specified Number of Unwelcome Communications did not cease within 5 Business Days of sending the initial warning letter, then:

(a) the A-Party Supplier must Suspend, or, if Suspension is not possible, Disconnect the A-Party Customer's Carriage Service within 2 Business Days of receiving the advice from the B-Party Supplier: and

(b) following the Suspension/Disconnection of the A-Party Carriage Service, formally advise the A-Party Customer in writing) within 5 Business Days that their Carriage Service has been Suspended/Disconnected as Unwelcome Communications to the Helpline have continued despite attempts to advise the A-Party Customer that the Unwelcome Communications must cease.

*NOTE: Refer to Appendix I for a suggested letter Suspending a Customer's service after further Unwelcome Communications to a Helpline following an initial warning letter.*

5.2.10 If the A-Party Customer contacts the A-Party Supplier in response to the Suspension/Disconnection of their Carriage Service, the A-Party Supplier may, at its discretion, reinstate the service, if the A-Party Customer provides a written undertaking within 10 Business Days that:

(a) the A-Party Customer understands the seriousness of the matter and that a crime may have been committed in relation to the use of the Carriage Service to offend, harass or menace another person; and

(b) this inappropriate use of the Carriage Service will not reoccur after the service is restored to normal operation, i.e., removal of the Suspension.

5.2.11 If the A-Party Supplier is not the B-Party Supplier, the A-Party Supplier must formally advise the B-Party Supplier in writing when the Suspension /Disconnection has been lifted upon receipt of the written undertaking from the A-Party Customer that the Unwelcome Communications to the Helpline will cease.

*NOTES: 1. Restoration or reconnection of a Carriage Service is at the discretion of the A-Party Supplier.*

*2.Not all Carriage Services have the ability to be Suspended, for some this will mean an immediate Disconnection of the Carriage Service.*

*3. Refer to Appendix J for a suggested letter to request restoration/reconnection of a Suspended/Disconnected Carriage Service.*

5.2.12 If the B-Party Supplier is not the A-Party Supplier, the B-Party Supplier must advise the A-Party Supplier that the Unwelcome Communications have continued to the Helpline after the notification of restoration/reconnection of the A-Party Customer's Carriage Service as per clause 5.2.11.

5.2.13 Where Unwelcome Communications have continued to the Helpline after the restoration/reconnection of the A-Party Customer's Carriage Service, the A-Party Supplier must:

(a) within 5 Business days, Disconnect the A-Party Customer's Carriage Service;

(b) engage with the A-Party Carrier to block the IMEI of the associated PMTS (in accordance with clause 5.2.15); and

(c) formally advise the A-Party Customer in writing within 2 Business Days that their Carriage Service has been Disconnected and the IMEI of their mobile device which was used for the Unwelcome Communications has been blocked across all mobile Carriers in Australia (in accordance with clause 5.2.15) in relation to Unwelcome

Communications to the Helpline having continued despite the written undertaking given by the A-Party Customer that the Unwelcome Communications to the Helpline would cease.

*NOTE: Refer to Appendix I for a suggested letter Disconnecting a Customer's service after further Unwelcome Communications to a Helpline following restoration of a Suspended service.*

5.2.14 The A-Party Supplier must ensure that the Disconnection process in clause 5.2.13 is completed within 5 Business Days of receiving the notification from the Helpline, or the B-Party Supplier under clause 5.2.9, and that the process does not have to start again if a delay occurs in the process.

5.2.15 Where the Specified Number of Unwelcome Communications to the Helpline originate via a PMTS from a mobile device, and following Disconnection of any associated PMTS, the associated IMEI of that device may be blocked across all mobile Carriers in Australia by the A-Party Supplier via the AMTA IMEI blocking process without prior warning.

*NOTES:*

1. *Where the B-Party Supplier is advised by the Helpline that it suspects that a large number of Unwelcome Communications are originating from a single mobile device, the B-Party Supplier should engage with the A-Party Supplier to facilitate the blocking of the IMEI used in Unwelcome Communications, via the A-Party Carrier.*

2. *Details of the AMTA blocking process are available from (www.amta.org.au).*

5.2.16 If, at any point under section 5, after an A-Party Supplier has:

(a) received an Unwelcome Communication action request from a B-Party Supplier;

(b) verified there has been a Specified Number of Unwelcome Communications, or has relied on evidence from the B-Party Supplier showing this;

(c) considered the evidence and circumstances, in consultation with the Helpline; and

(d) identified that there are either:

i) extenuating circumstances that caused the Unwelcome Communications; or

ii) other matters indicating that taking the relevant action would have an unacceptable and/or detrimental impact on the Customer, or others,

(e) then the A-Party Supplier may:

i) find that the Customer did not make the Unwelcome Communications and that no further action is necessary;

ii) find that the Customer has taken adequate steps to prevent further Unwelcome Communications occurring; or

iii) decide that taking the action under section 5 would have an unacceptable and/or detrimental impact on the Customer, or others,

(f) and consequent upon a finding or decision in (e) above, the A-Party Supplier may choose to either:

i) delay taking the relevant action;

ii) not take the relevant action under section 5; or

iii) take another action.

5.2.17 If the A-Party Supplier proceeds under clause 5.2.16(f):

(a) the A-Party Supplier should notify the B-Party Supplier within two Business Days after receiving the Unwelcome Communications action request, and provide details of the extenuating circumstances or other matters identified in clause 5.2.16; and

(b) the A-Party and/or B-Party Supplier must agree who will contact the Helpline, and within three Business Days of the notification in clause 5.2.17(a), the relevant Supplier must provide the Helpline with details identified in clause 5.2.16, and request the Helpline's advice on the handling of the matter seeking the Helpline's written agreement to the A-Party Supplier:

i) delaying taking the relevant action;

ii) not taking the relevant action under section 5; or

iii) taking another action in consultation with the Helpline.

(c) If the details identified in clause 5.2.16 include sensitive information about the B-Party Customer or others as defined in the Privacy Act, the B-Party Supplier must obtain the B-Party Customer's consent to disclose the details to the A-Party Supplier and the Helpline in accordance with subclauses (a) and (b) above.

*NOTES:*

1. *For the purposes of time limits/requirements in this Code, the passing of time is considered to be paused in relation to the Unwelcome Communications matter, from the time the A-*

*Party Supplier notifies the B-Party Supplier under clause 5.2.17(a).*

2. *After the B-Party Supplier has been notified under clause 5.2.17(a), the A-Party Supplier may also contact the relevant Helpline directly if agreed with the B-Party Supplier under 5.2.17 (b).*

3. *The Helpline is expected to respond to the request for input under clause (b)within 5 Business Days of receiving the request from the relevant Supplier.*

4. *Unacceptable and/or detrimental impacts include but are not limited to those where taking an action under section 5 could cause significant harm to the Customer, other people (e.g., the Customer's family members) or the community.*

5. *Ongoing Unwelcome Communications, occurring over an extended period of time, are not excused by the circumstances set out in clause 5.2.16(d).*

6. *Taking another action may include escalating the matter to the Police, and/or limiting the communication capabilities of the Customer, in consultation with other parties involved in the matter.*

5.2.18 If the Helpline does not provide written agreement under clause 5.2.17 (b), the A-Party Supplier must consider the most appropriate course of action in the circumstances and ensure that, as far as practicable, any solution has the effect of stopping Unwelcome Communications to the Helpline.

5.2.19 All communications between the A-Party Supplier, B-Party Supplier and / or the Helpline must meet applicable privacy requirements.

5.2.20 To effectively manage Unwelcome Communications for Customers, it is recommended that Suppliers retain, where practicable:

(a) Communications Records of communications made or received by the Customer subject to the Unwelcome Communication for a period of at least 30 days following the initial contact made by the Customer; and

(b) records of all other communications with that Customer relating to their Unwelcome Communications for a period of at least three years after the last communication with the Customer.

5.2.21 Where the Supplier has had no referrals of Unwelcome Communications relating to the CSI of the A-Party Customer for the previous three years to the same Helpline, the warning letter process for an A-Party Customer must begin again in the event there are further Unwelcome Communications. The matter will be treated as a new case with no precedents to be taken into

account irrespective of the stage at which a prior process had reached for a different Helpline.

5.2.22 In the event there were Unwelcome Communications within the previous three years from an A-Party Customer to the same Helpline, the process for an A-Party Customer must be treated as continuation of the previous case and will continue from the stage at which a prior process had reached.

# 6 UNWELCOME COMMUNICATIONS TO THE ECS

## Summary

Unwelcome Communications to the ECS may involve threat, menace, harassment or cause offence and have the potential to have a higher negative impact to the community than Unwelcome Communications to a single consumer of communications services. Due to the nature of the ECS and the need to respond to genuine emergencies, Unwelcome Communications to the ECS require time critical responses by Suppliers to investigate and take action to halt or hinder communications that involve threat, menace, harassment or cause offence.

It is generally recognised that the impact of Unwelcome Communications to the ECS can fall into two categories:

- can cause problems in the ability for genuine users of the services to gain access to help they may need to lessen or prevent injury or loss of life especially where the volume of communications to the ECS is of concern and could have the effect of potentially emulating a Denial of Service (DoS) attack; and

- can cause psychological trauma to the ECS call-takers who may be unable to continue to perform their duties and could require counselling.

*This section requires Suppliers to:*

- *assist the Emergency Call Person for 000 and 112 to manage Unwelcome Communications to the Emergency Call Service; and*

- *minimise Unwelcome Communications from a mobile device to the ECS.*

## Objectives

*The objectives of this section are to:*

- *describe the process for the handling of Unwelcome Communications to the ECS; and*

- *describe the process to minimise Unwelcome Communications from a mobile device to the ECS.*

### 6.1 General

6.1.1 All Suppliers that are engaged by the ECP for 000 and 112 in relation to Unwelcome Communications that have been made to the ECS from a PMTS must assist by:

(a) entering details in the customer's records that warnings have been issued to the A-Party MSN by the ECP to advise that a specified number of Unwelcome Communications have originated from that Carriage Service for which they are responsible and that, if the Unwelcome

Communications continue, the Carriage Service may be Suspended or Disconnected;

(b) Suspending the Carriage Service from which a specified number of Unwelcome Communications have continued to the ECS after warnings have been issued; or

(c) Disconnecting the Carriage Service from which a specified number of Unwelcome Communications have continued to the ECS after warnings have been issued and a warning letter has been issued by the Supplier of the Carriage Service.

*NOTE: Examples of warnings include a phone call from the ECP, a SMS from the ECP or Police attendance.*

## 6.2 Processes in Response to Unwelcome Communications to the ECS

6.2.1 The ACMA must, by notice in writing given to all Suppliers and the ECP for 000 and 112, communicate the number of Unwelcome Communications to the ECP for 000 and 112 over a specified period of time ("the specified number"), as agreed between the ACMA, the ECP for 000 and 112 and Carriers from time to time, that will trigger action in the following clauses.

6.2.2 Subsequent to the receipt of the specified number of Unwelcome Communications to 000/112 from a PMTS, the ECP must attempt to contact the A-Party to educate the Customer about the appropriate use of 000/112 and that improper use of the ECS is a criminal offence.

*NOTE: It is an offence under Section 474.18 of the Criminal Code Act 1995 to make improper use of ECS.*

6.2.3 Where Unwelcome Communications to the ECS continue, the ECP must:

(a) send a warning SMS to the A-Party MSN to alert the Customer that the Carriage Service has been used for an illegal activity;

(b) enlist the support of Police to attend the physical address of the Customer of the A-Party Carriage Service to alert them to the commission of a crime;

(c) send a second warning SMS to the A-Party MSN prior to requesting Suspension or Disconnection of the service, where the ECP has not received a response from Police within 5 Business Days regarding Police action taken.

6.2.4 If Unwelcome Communications to the ECS continue, the ECP must, subject to clause 6.2.3(c), request that the Supplier either:

(a) Suspend the A-Party Carriage Service and formally advise the Customer in writing that their Carriage Service will not

be restored until such time as they affirm that improper use of the ECS will stop; or

(b) Disconnect the A-Party Carriage Service and formally advise the Customer in writing that their Carriage Service will not be restored as Unwelcome Communications to the ECS have continued despite numerous attempts by the ECP and the Supplier to advise the Customer that the Unwelcome Communications must stop.

6.2.5 If a Supplier has Suspended a Carriage Service and the Unwelcome Communications to the ECS continue, the Supplier must Disconnect the Carriage Service.

6.2.6 Where Unwelcome Communications have continued to the ECS from a PMTS after that Carriage Service has been Disconnected, the IMEI of the device that has been used to make Unwelcome Communications to the ECS must be blocked across all mobile Carriers in Australia via the Australian Mobile Telecommunications Association (AMTA) Clearing House (refer to Appendix K).

6.2.7 Where the specified number of Unwelcome Communications to the ECS have originated from a mobile device and no Supplier is able to identify a CSI related to that mobile device, the associated IMEI of that device will be blocked across all mobile carriers in Australia via the AMTA Clearing House without prior warning (refer to Appendix K).

# 7 CONTACT POINTS

## Summary

*This section requires Suppliers to:*

- *maintain a point of contact for the management of Life-Threatening Communications around the clock; and*
- *maintain a point of contact for the management of Unwelcome Communications.*

## Objectives

*The objectives of this section are to:*

- *oblige Suppliers to maintain contact points; and*
- *describe the essential information to populate and maintain an industry list of contacts.*

### 7.1 Contact Point for Life Threatening Communications

7.1.1 Each Supplier and the NRSP must appoint one organisational element, called the CTCC in this Code, to be the single point of contact for the management of Communication Traces related to Life Threatening Communications. The CTCC must be available 24 hours a day, 7 days per week.

7.1.2 All Suppliers and the NRSP must ensure that they have supplied and keep up to date the following information to Communications Alliance and the nominated contact point within their CTCC:

(a) a 24 hour a day, 7 days a week contact Public Number for the provision of Communications Trace and Customer information in relation to Life Threatening Communications. This contact Public Number must be answered without unreasonable delay;

(b) details of an escalation contact that is available 24 hours a day, 7 days a week; and

(c) a business hours contact name and Public Number for arranging routine tests of Communications Tracing.

*NOTE: Communications Alliance will maintain an industry list with the contact information for Life Threatening Communications. Communications Alliance will periodically engage those nominated representatives to ensure that the list is accurate.*

7.1.3 All Suppliers and the NRSP must notify Communications Alliance, in writing, within 24 hours of changes to the information previously provided under clause 7.1.2.

*NOTE: On receiving the notification Communications Alliance will endeavour to confirm receipt in writing of the notification within 2 Business Days.*

7.1.4 All Suppliers must make the latest Communications Alliance Supplier contact list and PCC list readily accessible to all appropriate staff in their CTCC.

## 7.2 Contact Point for Unwelcome Communications

7.2.1 All Suppliers and the NRSP must supply Communications Alliance with their nominated contact point for Unwelcome Communication complaints and keep that information current. Details include:

(a) a contact name and Public Number for liaison in relation to Unwelcome Communication complaints; or

(b) a business hours contact name and Public Number for arranging the tracing of the source of an Unwelcome Communication; and

(c) a business hours contact name and email address for the provision of secure access to the Helpline register.

*NOTE: Communications Alliance will maintain an industry list with the contact information for Unwelcome Communications that will only be available to nominated representatives of all Suppliers.*

7.2.2 All Suppliers and the NRSP must notify Communications Alliance of any changes to their nominated contacts, in writing, within 10 Business Days of any changes to that information.

# 8 COMMUNICATIONS TRACING

## Summary

*This section requires Suppliers to:*

- *have arrangements to ensure the ongoing ability to identify the source of a communication; and*
- *allocate Dummy CSIs where an A-Party CSI is not available.*

## Objectives

*The objectives of this section are to:*

- *set out the minimum requirements for Communications Tracing; and*
- *provide information related to Dummy CSIs.*

### 8.1 General

8.1.1 Communications Tracing between Suppliers must be undertaken using agreed standards, for example voice calls currently use Common Channel Signalling (CCS) System No. 7.

8.1.2 Requests for Communications Tracing of communications in progress with an unknown A-Party between Suppliers must include the Interconnect Route Name and Circuit Identification Code (CIC) where available.

### 8.2 Dummy CSIs

8.2.1 Suppliers using Dummy CSIs must be able to determine the source network.

8.2.2 In accordance with the provisions of inter-Carrier agreements, Australian Carriers must allocate Dummy CSIs where an A-Party CSI is not available (e.g., calls entering Australia from an overseas country).

*NOTE: Examples of some Dummy CSIs can be found in ACIF G549. This information is required to communicate the origin of a call between interconnecting carriers. For further information on Dummy CSIs, see Appendix L.*

### 8.3 Ongoing Arrangements

8.3.1 Suppliers must have arrangements to ensure the ongoing ability to identify the source of a communication. This may include making test communications with other Suppliers and, if appropriate, the NRSP, to identify the A-Party of the test communication.

# 9 REFERENCES

| Publication | Title |
|---|---|
| **Industry Codes** | |
| C609 | Priority Assistance for Life Threatening Medical Conditions |
| C536 | Emergency Call Services Requirements |
| C661 | Reducing Scam Calls and Scam SMs |
| **Industry Guidelines** | |
| ACIF G500:2000 | Signalling System No. 7 - Interconnection ISUP |
| ACIF G549:2000 | Interconnection Implementation Plan |
| G660 | Assisting Customers Experiencing Domestic and Family Violence |
| IGN010 | Customer Process – Handling of Life Threatening and Unwelcome Communications |
| **Legislation** | |
| *Criminal Code Act 1995* | |
| *Do Not Call Register Act 2006* | |
| *Privacy Act 1988* | |
| *Spam Act 2003* | |
| *Telecommunications Act 1997* | |
| *Telecommunications (Consumer Protection and Service Standards) Act 1999* | |
| *Telecommunications (Interception and Access) Act 1979* | |
| *Telecommunications (Emergency Call Service) Determination 2019* | |
| *Telecommunications Numbering Plan 2015* | |

# APPENDICES

## A LIFE THREATENING CALL TRACE PROCESS

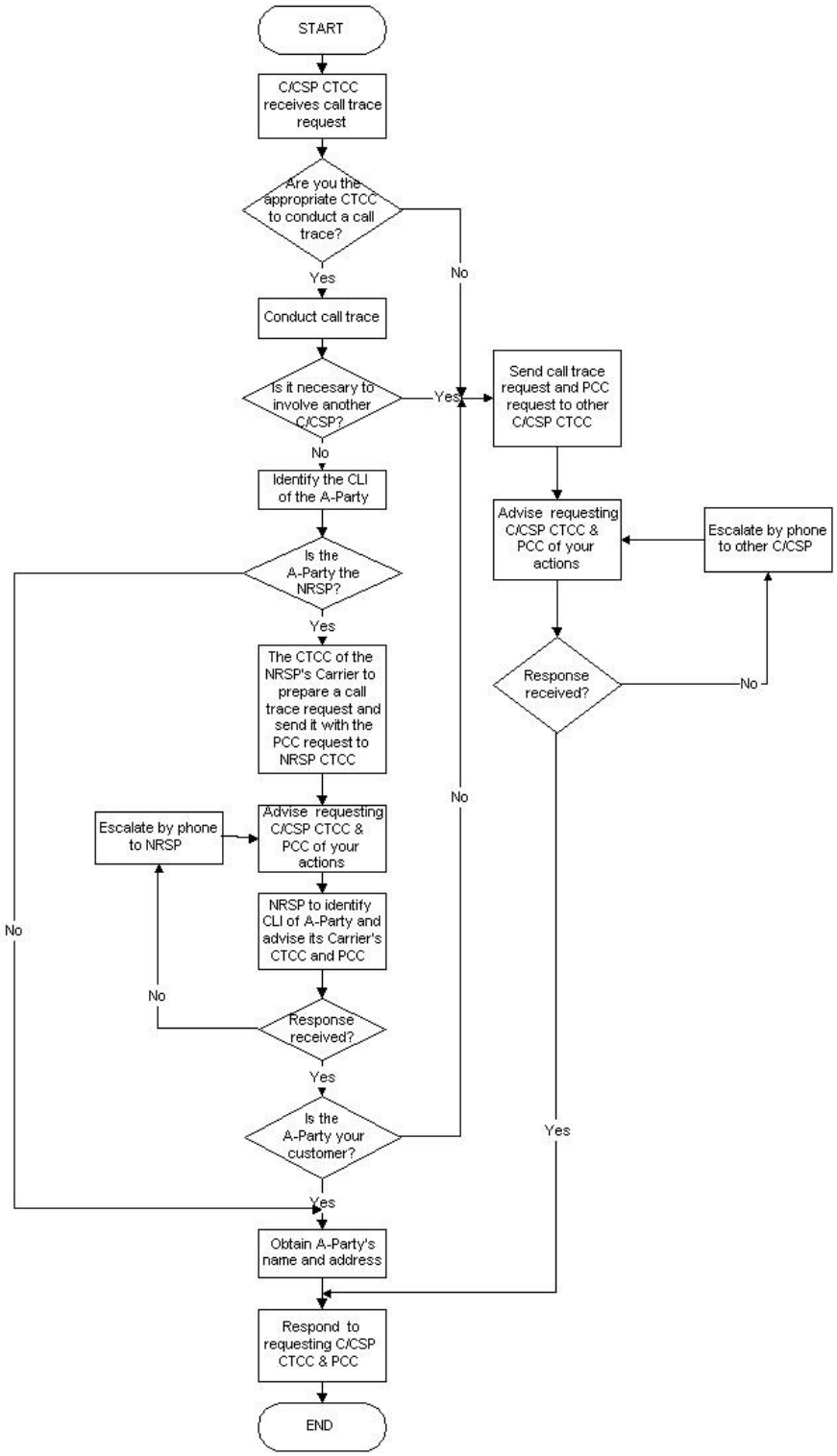



**FIGURE 1**
**Life Threatening Call Trace Process**

# B PCC REQUEST FORM

**Identification details of**
**Police Communications Centre (PCC)**

***Your Logo here***

**Name of Carrier / Service Provider:** _____

| | | | |
|---|---|---|---|
| **Please Arrange For:** | | CCR/RCCR ..... | ☐ |
| Emergency Life Threatening Trace | ☐ | Implement Call Trace Facility..... | ☐ |
| Mobile Location ..... | ☐ | Customer Details (Life Threatening only) | ☐ |

**of Telephone Number:** _____

**Brief Details including date, time and duration of subject calls:**

_____

_____

_____

**Police Communication Centre to complete:**

**Police Reference Number:** _____ **Date:** ___/___/_____ **Time:** ____: ____

I certify that this request is reasonably necessary in accordance with Section 287 *Telecommunications Act 1997* - To prevent or lessen a serious threat to life or health of a person.

**Officer Requesting:** _____ _____ _____

(Print Name) (Signature) (Rank)

**Relevant Carrier / Service Provider to complete:**

**CALL TRACE RESULT** ☐ **CALL TRACE UNSUCCESSFUL** ☐

**Originating Number (A-Party):** _____

**Customer Name:** _____

**Customer Address:** _____

_____

**CTCC Sequence No.:** _____

**CTCC Officer:**

_____ _____ _____ ___/___/_____ ____:____

(Print Name) (Signature) (Contact number) (Date) (Time)

# C INTERCONNECT REQUEST FOR CALL TRACE FORM

**1. Important**, Tick as appropriate.

Emergency Life Threatening. .....(Police initiated) ☐ (C/CSP initiated) ☐

Is the call in progress ..... Yes ☐ No ☐

Is the Police trace request attached ..... Yes ☐ No ☐

**2. The CTCC initiating the trace:** _____ ___/___/_____ ____: ____

(Carrier) (Date) (Time)

_____ _____ _____ _____

(Print Name) (Signature) (Contact Number) (Fax number)

I certify that the information sought is required under the disclosure of information provisions of the Telecommunications Act 1997 (Cth)

**3. Called number (B-Party) receiving life threat call.**

**Terminating Number:** _____

Call establishment details ___/___/_____ ____: ____

(Date) (Time)

Enter if A-Party details known for life threat call. Originating Number: _____

Which carrier does this originating number belong to. Carrier: _____

**4. Note: Only enter details for CIC and route if originating (A) number is unknown.**

| Organisation | Contact Number | CIC | Route |
|---|---|---|---|
| 1 | | | |
| 2 | | | |
| 3 | | | |
| 4 | | | |

**5. Call Trace Results:**

**Originating Number (A-Party):** _____

**Important,**

- **Customer name and address is provided, if available, for Life Threatening only**
- **If the customer name and address is not available, note the reason in the comment box below**

Customer Name: _____

Customer Address: _____

The Carrier providing customers details: _____ _____

(Organisation) (Print Name)

_____ _____ _____ ___/___/_____ ____:____

(Signature) (Contact Number) (Fax number) (Date) (Time)

Has the PCC been advised by Phone and Fax .....Yes ☐ No ☐

**6. Comments:** _____

**Notes: PCC = Police Communications Centre. CTCC = Call Trace Coordination Centre**
**Details must be supplied when this request is received from an appropriate CTCC.**
**Steps 1, 2 &3 are entered by the originating CTCC, step 4 by the originating and/or transit CTCC & step 5 by final CTCC.**

# D UNWELCOME COMMUNICATIONS TRACE PROCESS

## D1 Unwelcome Communications Trace Flowchart For A-Party CSP (excluding Domestic and Family Violence (cl 4.4.18) and Helpline (section 5) situations).

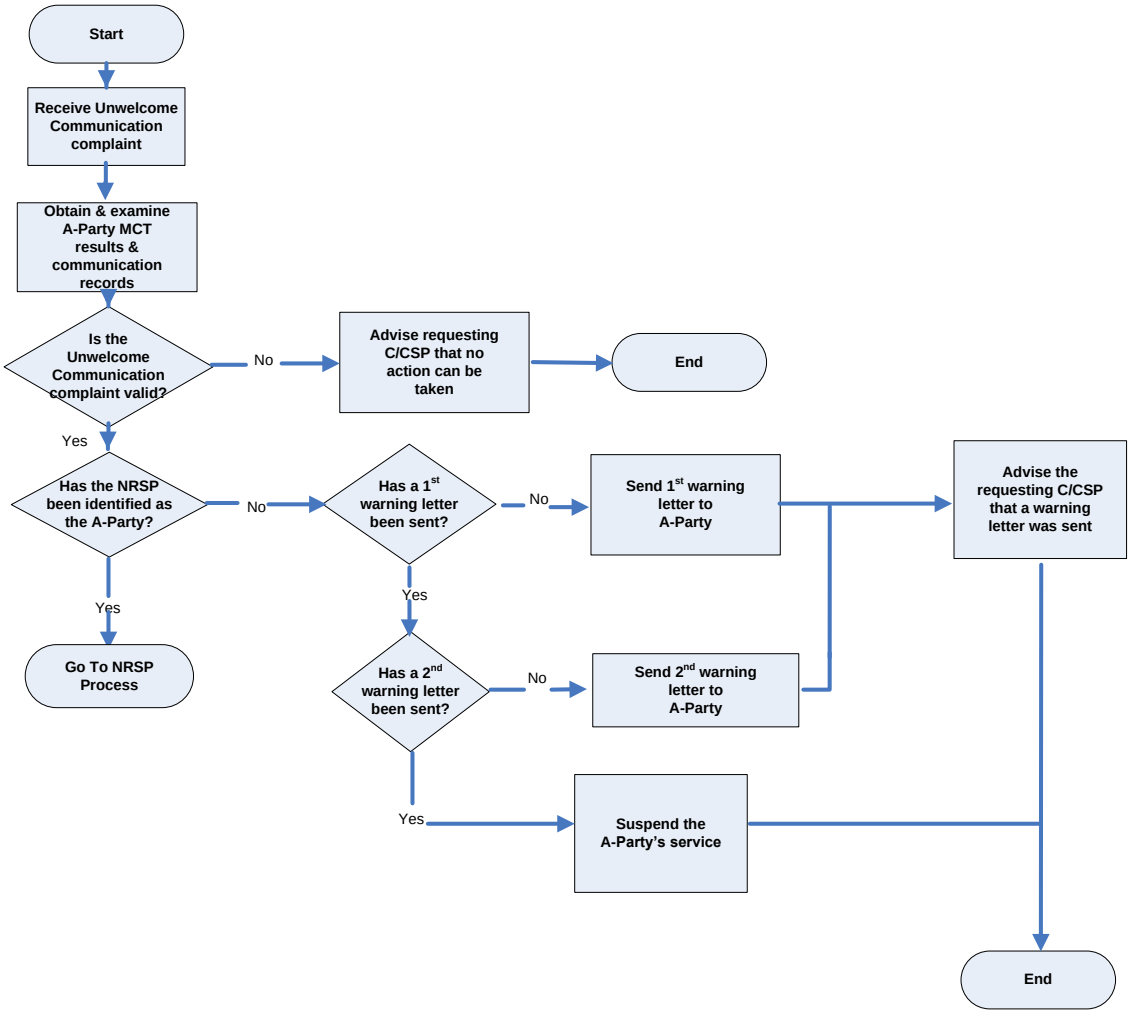



**FIGURE 2**

**Unwelcome Communications Trace Flowchart For A-Party CSP**

## D2 Unwelcome Communications Trace Flowchart For B-Party CSP (excluding Domestic and Family Violence (cl 4.4.18) and Helpline (section 5) situations).

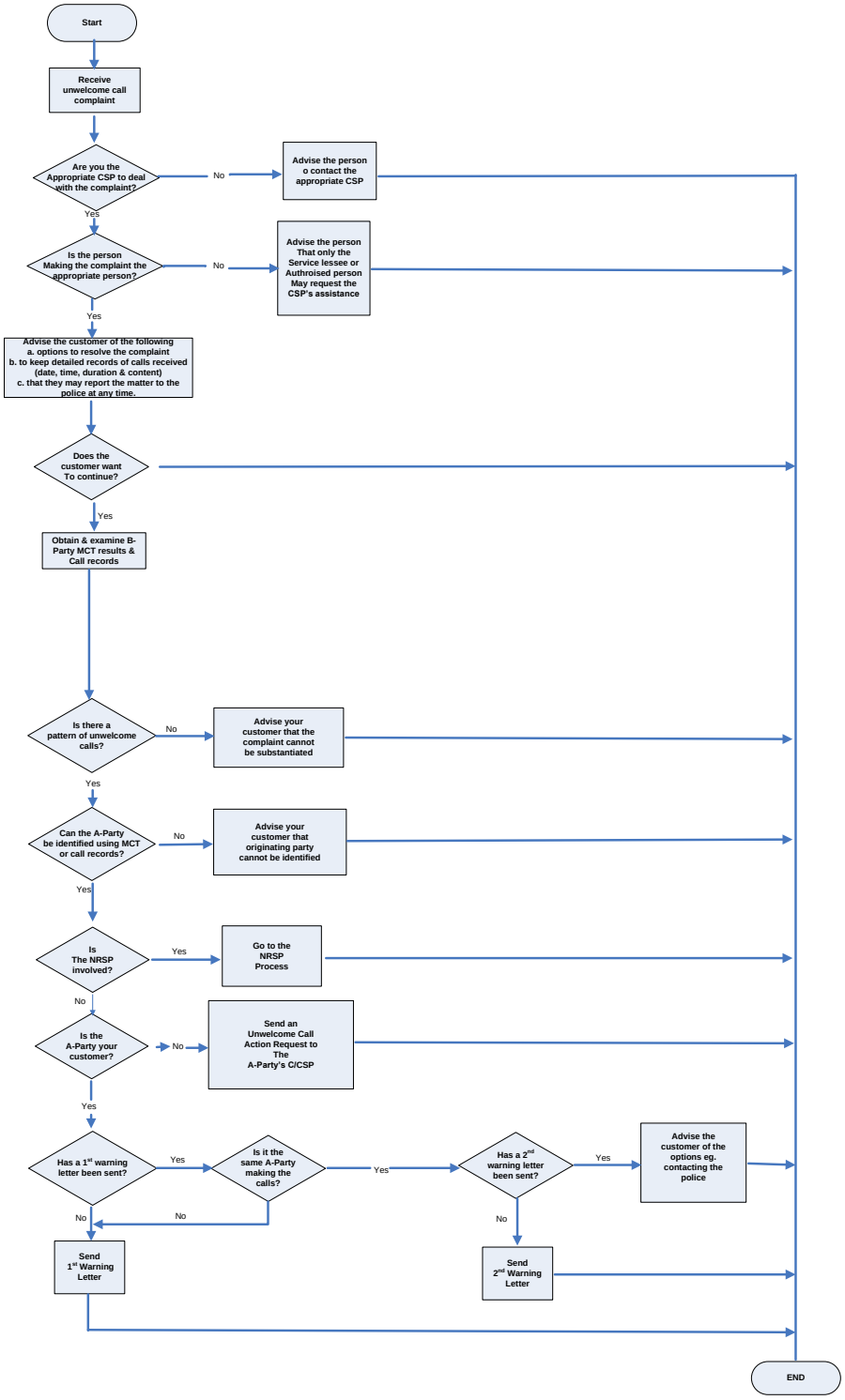



**FIGURE 3**

**Unwelcome Communications Trace Flowchart For B-Party CSP**

# D3 Unwelcome Communications Trace Flowchart For NRSP

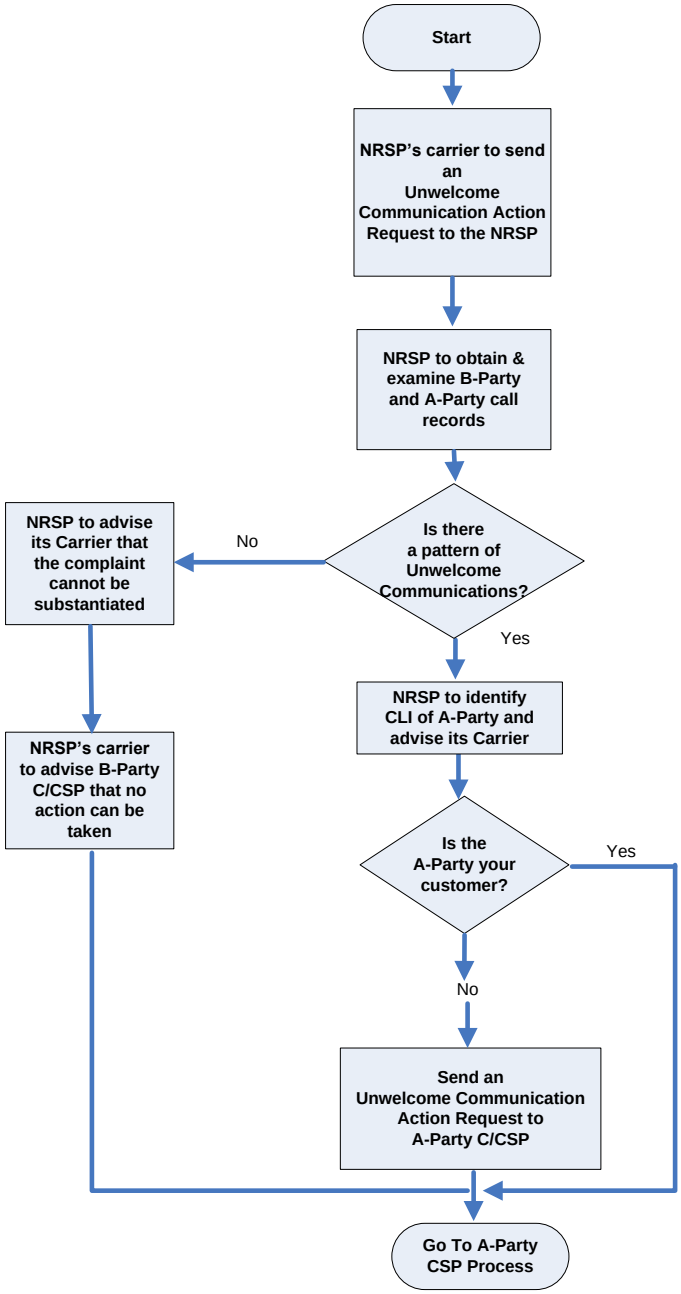



**FIGURE 4**

**Unwelcome Communications Trace Flowchart For NRSP**

# E REQUEST FROM POLICE FOR ASSISTANCE WITH UNWELCOME COMMUNICATIONS INVESTIGATION

(POLICE LETTERHEAD)

OUR REFERENCE:

DATE:

TO: UNWELCOME COMMUNICATIONS INVESTIGATION UNIT

<<insert Carrier's name>>

Dear Sir/Madam

I am writing to notify you of a complaint received from {Mr/Mrs} <<insert name of complainant>> of <<insert address of complainant>> regarding Unwelcome Communications being received on service <<insert telephone number/service receiving Unwelcome Communications>>.

The complainant has expressed a desire that <<insert Carrier's name>> provide all assistance possible, to resolve this matter.

I further certify that I am investigating this complaint as an alleged breach of section 474.17 of the *Criminal Code Act 1995*. [Optional condition - Accordingly I request that << insert Carrier's name>> does not proceed with its normal warning letter process.]

The dates and times of the Unwelcome Communications quoted by the complainant are listed below:

Signed: …….. Name: ……..

Contact Number: …… Rank: ……..

# F SUGGESTED UNWELCOME COMMUNICATIONS ACTION REQUEST

| | |
|---|---|
| CSI to which Unwelcome Communications have been made | *[e.g., Mobile Number and IMEI]*<br>*[For a Helpline, include the name of the Helpline, and Helpline dispute resolution contact details as provided by the Helpline]* |
| Details of Unwelcome Communications | *[Dates and times and the suspected identity or CSI of the unwelcome communicator if known]* |
| Action taken | *[eg. contacting Police]* |

*Select from the following:*

*[B-Party Supplier]* requests that *[A-Party Supplier]* inspect its Communications Records in relation to Unwelcome Communications detailed above to determine if there is a Pattern of Unwelcome Communications *[or the Specified Number of Unwelcome Communications have occurred – in the case of a Helpline]*

*[A-Party Supplier]* should inform *[B-Party Supplier]* from time to time of the progress of the investigation.

OR

*[NRSP's Carrier]* requests the NRSP to:

(a) inspect its Communications Records of the B-Party and A-Party in relation to the Unwelcome Communications detailed above to determine if there is a pattern of Unwelcome Communications. If the claim can be substantiated, then issue a warning letter to its Customer; and

(b) release the CSI and IMEI of the A-Party to its Carrier if a pattern of communications is identified.

Contact Name: _____

Contact Number: _____

Signed: _____

Date: _____

# G SUGGESTED INITIAL WARNING LETTER

## G1 Initial Warning Letter

Dear *[Customer name]*

We have recently been contacted by *[one of our Customers/another Carrier/a Carriage Service Provider]* * regarding Unwelcome Communications being received from your service(s) [insert service identifier(s)].

The term "Unwelcome Communications" is defined in Communications Alliance C525:2023 Handling of Life Threatening and Unwelcome Communications Industry Code ("the Code") which is accessible on Communications Alliance website at URL: http://www.commsalliance.com.au/Documents/all/codes/c525

Subsequent analysis shows that the following Unwelcome Communications were received by that *[Customer/Carrier's Customer/Carriage Service Provider's Customer]* *. Our records show that these Unwelcome Communications originated from your service(s) [List CSI(s) here].

| **Date** | **Time** | **Called Party Service identifier** (tel. no., email address, etc.) |
|---|---|---|
| DD/MM/YY | hh:mm | |
| DD/MM/YY | hh:mm | |

We wish to bring to your attention that it is an offence under section 474.17 of the Criminal Code Act 1995 to use a telephone service to menace or harass, or to make communications which may be considered offensive.

While [Supplier name] does not wish to imply that there was any intention to make Unwelcome Communications of this nature, or that you personally made those Unwelcome Communications, you as the responsible party for the service(s) must ensure that the service(s) is / are not used to commit an offence and we expect your cooperation to ensure that your service(s) is/are not used to make Unwelcome Communications in the future.

Please contact us on telephone number (  )  if you would like to discuss this matter further.

Yours sincerely

.....

[Name]

[Title]

* *Delete incorrect option*

## G2 Initial Warning Letter_HELPLINE

Dear [Customer name]

We have recently been contacted by [Helpline] regarding Unwelcome Communications being received from your service(s) [insert service identifier(s)].

The term "Unwelcome Communications" is defined in Communications Alliance C525:2023 Handling of Life Threatening and Unwelcome Communications Industry Code ("the Code") which is accessible on Communications Alliance website at URL: http://www.commsalliance.com.au/Documents/all/codes/c525

Subsequent analysis shows that the following Unwelcome Communications were received by [Helpline]. Our records show that these Unwelcome Communications originated from your service(s) [List CSI(s) here].

| **Date** | **Time** | **Called Party Service identifier** (tel. no., email address, etc.) |
|---|---|---|
| DD/MM/YY | hh:mm | |
| DD/MM/YY | hh:mm | |

We wish to bring to your attention that it is an offence under section 474.17 of the *Criminal Code Act 1995* to use a telephone service to menace or harass, or to make communications which may be considered offensive.

While [Supplier name] does not wish to imply that there was any intention to make Unwelcome Communications of this nature, or that you personally made those Unwelcome Communications, you as the responsible party for the service(s) must ensure that the service(s) is / are not used to commit an offence. We expect your cooperation to ensure that your service(s) is/are not used to make Unwelcome Communications in the future.

If you dispute that these communications with [Helpline] were Unwelcome Communications, please contact [Helpline] dispute resolution team to discuss the matter further.

You should also be aware that if any further complaints are received from [Helpline], your service will be suspended or disconnected without any further notice as per section 5 of the Code, the Unwelcome Communications could become the subject of a Police investigation, and the IMEI of the mobile device that was used for the Unwelcome Communications may be blocked across all mobile Carriers in Australia resulting in an inability to make or receive calls from that mobile device.

Yours sincerely

.....

[Name]

[Title]

# G3 Initial Warning Letter_Domestic and Family Violence

Dear *[Customer name]*

We have recently been contacted by *[one of our Customers/another Carrier/a Carriage Service Provider]* * regarding Unwelcome Communications being received from your service(s) [insert service identifier(s)].

The term "Unwelcome Communications" is defined in Communications Alliance C525:2023 Handling of Life Threatening and Unwelcome Communications Industry Code ("the Code") which is accessible on Communications Alliance website at URL: http://www.commsalliance.com.au/Documents/all/codes/c525

Subsequent analysis shows that the following Unwelcome Communications were received by that *[Customer/Carrier's Customer/Carriage Service Provider's Customer]* *. Our records show that these Unwelcome Communications originated from your service(s) [List CSI(s) here].

| **Date** | **Time** | **Called Party Service identifier** (tel. no., email address, etc.) |
|---|---|---|
| DD/MM/YY | hh:mm | |
| DD/MM/YY | hh:mm | |

We wish to bring to your attention that it is an offence under section 474.17 of the Criminal Code Act 1995 to use a telephone service to menace or harass, or to make communications which may be considered offensive.

While [Supplier name] does not wish to imply that there was any intention to make Unwelcome Communications of this nature, or that you personally made those Unwelcome Communications, you as the responsible party for the service(s) must ensure that the service(s) is / are not used to commit an offence and we expect your cooperation to ensure that your service(s) is/are not used to make Unwelcome Communications in the future.

You should also be aware that if any further complaints are received regarding Unwelcome Communications, your service will be suspended or disconnected without any further notice as per clause 4.4.18 of the Code, the Unwelcome Communications could become the subject of a Police investigation, and the IMEI of the mobile device that was used for the Unwelcome Communications may be blocked across all mobile Carriers in Australia resulting in an inability to make or receive calls from that mobile device.

Please contact us on telephone number ( ) if you would like to discuss this matter further.

Yours sincerely

.....

[Name]

[Title]

* *Delete incorrect option*

# H SUGGESTED SECOND WARNING LETTER

## H1 Second Warning Letter

Dear

I refer to my previous letter dated DD MONTH YEAR regarding Unwelcome Communications originating from your service(s).

Since that date, further Unwelcome Communication(s) have been received from your service(s) [insert service identifier(s)]. Our analysis shows the following Unwelcome Communications have been made from your service(s).

| **Date** | **Time** | **Called Party Service identifier** (tel. no., email address, etc.) |
|---|---|---|
| DD/MM/YY | hh:mm | |
| DD/MM/YY | hh:mm | |

I wish to bring to your attention that it is an offence under section 474.17 of the *Criminal Code Act 1995* to use a telephone service to menace or harass, or to make communications which may be considered offensive.

You should be aware that if any further complaints are received, your service(s) will be suspended or disconnected and the Unwelcome Communications could become the subject of a Police investigation.

If you would like to discuss any aspect of this matter further, please contact us on

( ) _____ .

Yours sincerely

.....

[Name]

[Title]

# I SUGGESTED LETTER FOR SUSPENSION OR DISCONNECTION OF A SERVICE

*NOTE: This template is only supplied as a guide. Suppliers will need to make appropriate modifications before using this letter to deal with the Helpline processes described in section 5 or a Domestic and Family Violence situation as per clause 4.4.18.*

Dear [customer name]

I refer to my previous letter dated [insert date] regarding Unwelcome Communications originating from your service(s) [insert service identifier(s)].

Since that date further Unwelcome Communications have been received from your service(s). Analysis shows the following Unwelcome Communications have been made from your service(s):

**Date** **Time** **Service identifier** (telephone number, email address, etc.)

DD/MM/YYYY hh:mm

The Communications Alliance Ltd Industry Code C525:2023 Handling of Life Threatening and Unwelcome Communications ("the Code"), which is registered with the Australian Communications and Media Authority, requires [Supplier name] to suspend/disconnect service(s) that have continued to make Unwelcome Communications (as defined in the Code). Under clause [4.4.18,4.4.20,4.4.22, 5.2.9 or 5.2.13] of the Code your service(s) has/have been suspended/disconnected.

You should be aware that, in accordance with the Code, [Supplier name] requires written undertakings from you that Unwelcome Communications (as defined in the Code) will not be made from your service(s) [insert service identifier(s)], before your service(s) can be restored/reconnected. If these undertakings are not provided then [Supplier name] will, pursuant to clause [4.4.20], disconnect your service(s) [insert service identifiers(s)]/ cannot, pursuant to clause [4.4.20 or 5.2.10], reconnect your service(s). The IMEI of the mobile device which was used for Unwelcome Communications may also be blocked across all mobile Carriers in Australia resulting in an inability to make or receive calls from that mobile device.

Yours sincerely

_____

Name
Title

# J SUGGESTED LETTER TO REQUEST RESTORATION / RECONNECTION OF A SUSPENDED OR DISCONNECTED SERVICE

*NOTE: This template is only supplied as a guide. Suppliers will need to make appropriate modifications before using this letter to deal with the Helpline processes described in section 5 or a Domestic and Family Violence situation as per clause 4.4.18.*

Dear [customer name]

I refer to my previous letter dated [insert date] informing you that your service [insert service identifier(s)] was/were suspended/disconnected by [supplier name] on [insert date] under clause [4.4.18 or 5.2.9] of Communications Alliance Ltd Industry Code C525:2023 Handling of Life Threatening and Unwelcome Communications ("the Code").

In order to restore/reconnect your service(s) [CSP] requires your agreement to the undertakings below within 10 Business Days  If you agree with these undertakings, please sign where indicated and return this letter in the enclosed pre-addressed envelope.

Yours sincerely

_____
Name
Title

---

**UNDERTAKING**

I [Customer name] undertake to ensure that Unwelcome Communications (as defined in the Code) will not be made from any of my communication services(s) [insert service identifiers(s)].

I acknowledge that my communication service(s) will be disconnected immediately should Unwelcome Communications continue to be made after service restoration/reconnection and following such disconnection my communication service(s) cannot be reconnected and if the service(s) use(s) a telephone number(s) I will lose the right to use that/those telephone number(s).

_____
Signature

_____
Date

# K REDUCTION OF NON-GENUINE CALLS TO THE ECS

## K1 ECP Process – Reduction of Non-Genuine Calls to the ECS

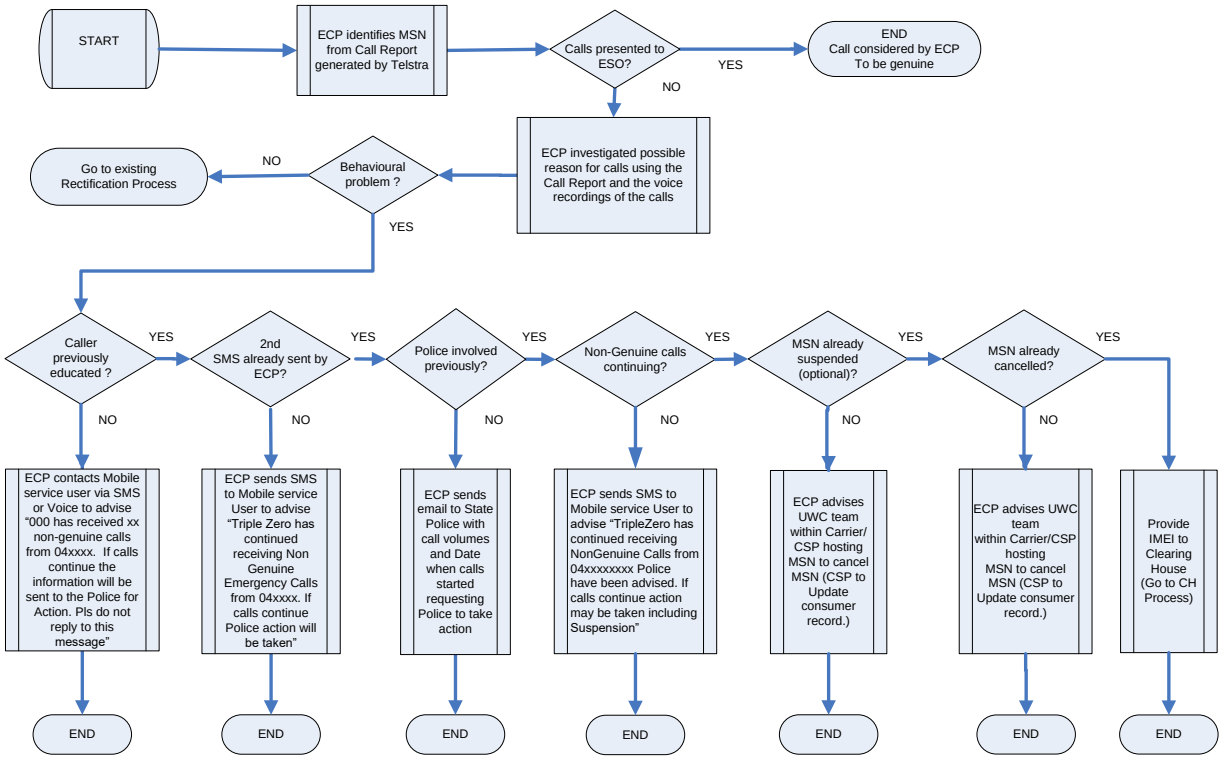



**FIGURE 5**

**ECP Process – Reduction of Non-Genuine Calls to the ECS**

NOTES:

1. ECP means Emergency Call Person for 000/112

2. UWC means Unwelcome Communications

3. SMS means Short Message Service

4. MSN means Mobile Service Number

5. CSP means Carriage Service Provider (Data Provider to Integrated Public Number Database.) Has the commercial relationship with the A-Party Customer of the service.

6. AMTA means Australian Mobile Telecommunications Association

7. IMEI means International Mobile Equipment Identifier (Hardware serial number of mobile handset.)

# K2 AMTA Clearing House Process – Reduction of Non-Genuine Calls to the ECS

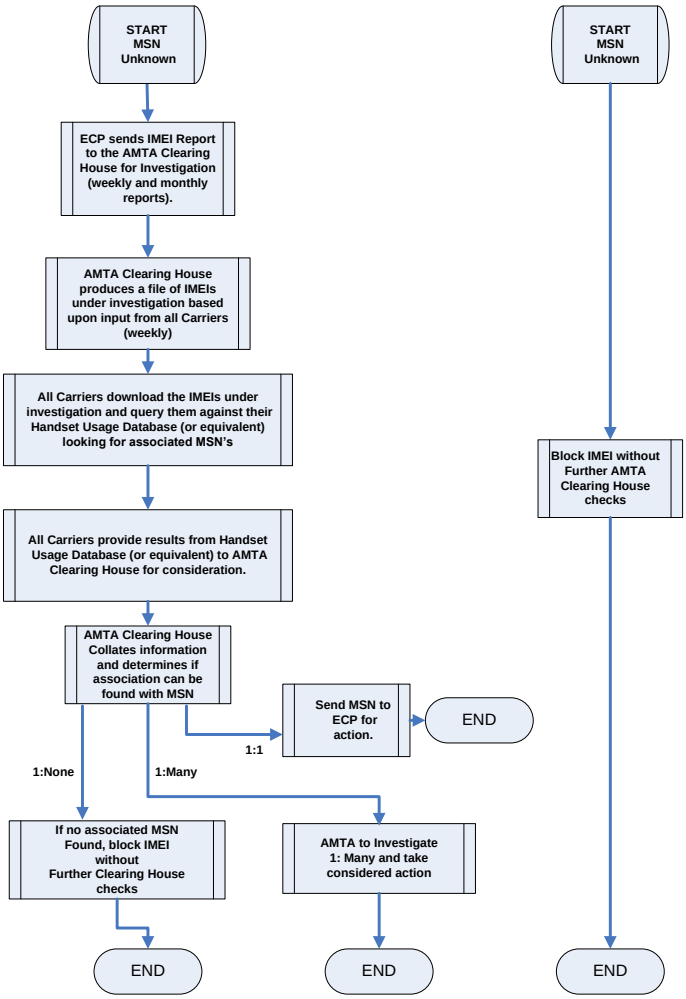



**FIGURE 6**

**AMTA Clearing House Process – Reduction of Non-Genuine Calls to the ECS**

# L DUMMY CSIs

Dummy CSIs are applied by Carriers to communicate to other Carriers the origin of the call. The following telephone traffic cases apply:

(a) National Origin Australia Terminating Customer Initiated Telephone Calls

(i) CCS Interconnected Carriers
The actual or true CSI is forwarded between networks so identification of the CSI of the calling party is readily available from the switch call data records.

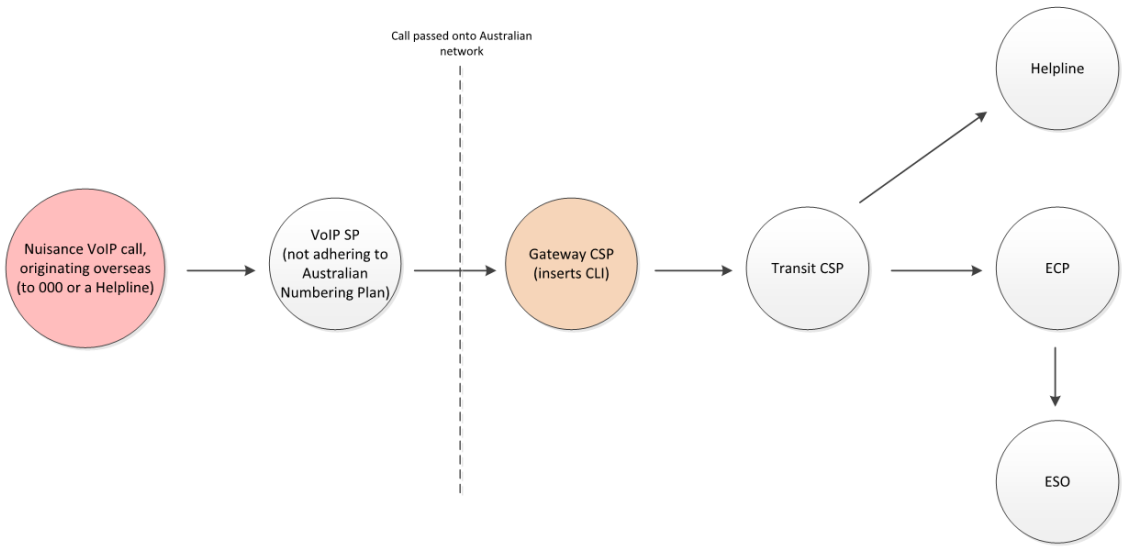
(ii) Non-CCS Interconnected Carriers
Such interconnected networks apply Dummy CSIs to facilitate identification of the origin of the call. Carriers receiving Dummy CSIs are unable to identify the actual or true CSI of the calling party.
In this case, the carrier receiving the call would need to contact the CTCC of the originating carrier to request identification.

(b) International Origin Australia Terminating Telephone Calls
According to convention, a Dummy CSI is applied by the carrier used as the point of entry for the call to Australia. The format of the Dummy CSI will conform to intercarrier agreements such as indicated in ACIF G549:2000 Interconnection Implementation Plan.

(c) National Origin International Terminating Telephone Calls
The carrier servicing the customer or the customer's C/CSP should block or clear the CSI of the calling party before the call is switched to another carrier's network. This is in accordance with international and intercarrier agreements that no calling party CSI should be transported over the international switching networks.

(d) National Origin Australia Terminating Operator Assisted Telephone Calls.

Nuisance VoIP calls originating overseas – call process



# PARTICIPANTS

The Working Committee responsible for the revisions made to this Code consisted of the following organisations and their representatives:

| Organisation | Representative | WC Membership |
|---|---|---|
| ACCAN | Wayne Hawkins | Voting |
| ACCAN | Elie Antonios | Non-voting |
| ACMA | Andrew Westmorland | Non-voting |
| Lifeline Australia | Amy Webster | Voting |
| nbn | Peter Bull | Voting |
| NSW Police Force | Kristy Walters | Voting |
| NSW Police Force | Kym Sharp | Non-voting |
| Optus | Warren Hudson | Voting |
| Telstra | Jane Elkington | Voting |
| Telstra | Fiona Wade | Voting |
| Telstra | Shannon Foster | Non-voting |
| TPG Telecom | Annie Leahy | Voting |
| TPG Telecom | Alexander R. Osborne | Non-voting |
| Vocus | John Sexton | Voting |

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

Communications Alliance was formed in 2006 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 25**
**100 Mount Street**
**North Sydney**
**NSW 2060 Australia**

**Correspondence**
**PO Box 444**
**Milsons Point**
**NSW 1565**

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