COMMUNICATIONS ALLIANCE LTD

INDUSTRY GUIDANCE NOTE IGN 010

CUSTOMER PROCESS – HANDLING OF LIFE THREATENING AND UNWELCOME COMMUNICATIONS

Customer Process – Handling of Life Threatening and Unwelcome Communications Industry Guidance Note IGN 010

Communications Alliance Ltd was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

Disclaimers

1. Despite anything contained in this Guidance Note:

   (a) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for any direct, indirect or consequential loss, damage, claim, or liability any person may incur as a result of any:

      (i) reliance on or compliance with this Guidance Note;

      (ii) inaccuracy or inappropriateness of this Guidance Note; or

      (iii) inconsistency of this Guidance Note with any law, Industry Code or Industry Guideline; and

   (b) Communications Alliance disclaims responsibility (including where Communications Alliance or any of its officers, employees, agents or contractors has been negligent) for ensuring compliance by any person with this Industry Guidance Note.

2. For avoidance of doubt:

   (a) You must not rely on the information in this document as an alternative to legal advice from your solicitor or other professional legal services provider.

   (b) You should never delay seeking legal advice, disregard legal advice, or commence or discontinue any legal action because of information in this document.

3. These disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

VERSION HISTORY

This document constitutes: Version 1 of Industry Guidance Note IGN 010

Date	Version	Comments/Changes
23/02/2017	1	First release
August 2022	2	Cl 4.2.6 amended to align with a revision of C525:2022

TABLE OF CONTENTS

1 BACKGROUND

In general, unwelcome communications are unsolicited communications that, by virtue of the content, frequency or timing, are offensive or tend to menace or 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 and imminent threat to a person's life or health.

To better 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.

2 OBJECTIVE OF THIS GUIDANCE NOTE

This Guidance Note is intended for customers and to provide guidance on the processes set out in the C525:2022 Handling of Life Threatening and Unwelcome Communications Industry Code (the Code) without the need to read the Code. The Guidance Note does not impose any additional obligations on service providers but is designed to explain key processes set out in the Code in lay terms and assist in the overall customer experience.

3 HANDLING OF LIFE THREATENING COMMUNICATIONS

3.1 What is a life-threatening communication?

A 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 and imminent 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 and imminent threat to the life or health of a person and may include, but is not limited to an event such as:
(a) a person being seriously injured,
(b) a bomb threat,
(c) an extortion demand,
(d) a kidnapping, or
(e) a threat to public safety.

3.2 What actions to take if you receive a life-threatening communication.

This Guidance Note outlines the steps consumers should take if they receive a life-threatening communication (e.g. via phone calls, SMS, MMS or email).

3.2.1 **Contact the police**

Life threatening communications should be reported to the police immediately. Where a telecommunications service has been used to threaten life or serious harm it may constitute a criminal offence under the Criminal Code Act 1995. For example, under section 474.15 of the Criminal Code Act 1995 it is a criminal offence if the communication is made to threaten to kill or to cause serious harm.

3.2.2 **Keeping Records**

You will need to provide what details you have of the:

- times and dates of any life-threatening communications,
- calling number or other reference used to identify the service (e.g. email address) if known, or can be identified.

These details are required to assist the service provider to implement protocols to deal with the threat.

If during the conversation your service provider believes on reasonable grounds that you have a serious and imminent threat against your life or health, your service provider should engage the police via a telephone call to 000 and release all information known about you that would be needed by police to dispatch emergency resources to meet the situation involving a life-

threatening communication. See also Section 5 – Reporting to the police

3.2.3 **Contact your service provider**

The police may refer you to your service provider in relation to an unwelcome communication. If this is the case, you should contact your service provider immediately to discuss the nature of the communication and its origin.

Your service provider will inform you on the unwelcome communications process. Section 4 of this Guidance Note provides information on this process.

4 HANDLING OF UNWELCOME COMMUNICATIONS

4.1 What is an unwelcome communication?

An unwelcome communication means the use of one or more types of communications service (e.g. voice, SMS/MMS or email) by a person to communicate with another person in a manner in which the receiving party advises is unwelcome but which is not currently a life-threatening communication.

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.

Under section 474.18 of the Criminal Code Act 1995, it is a criminal offence if the communication is made to the emergency call service (e.g. a call using 000): 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.

NOTE: For example, an unwelcome communication could be a repeated communication from an incorrectly programmed fax service or message bank service.

The definition of unwelcome communication includes:

(a) communications using one or more forms of carriage service. e.g. making calls from more than one public number used by the initiating party to one or more carriage services used by the receiving party;

(b) communications to the receiving party by one or more of the same type of carriage service used by the same receiving party e.g. unwelcome communications could include calls made to more than one public number used by that receiving party from a single source;

(c) use of a carriage service to make a call to the emergency call service that is non-genuine, malicious, vexatious or obscene; and

(d) improper use of the emergency call service.

4.2 What actions to take if you receive unwelcome communications.

If you have received one or two unwelcome communications your service provider may be limited in its ability to assist.

However, if you have received a pattern of unwelcome communications (e.g. via phone calls, SMS, MMS or email), there are set protocols established under the Code that sets out how service providers are to deal with these.

4.2.1 **What is a pattern of unwelcome communications?**

A pattern of unwelcome communications means:

(a) ten or more unwelcome communications in a 24-hour period;

(b) three or more unwelcome communications that are spread over a period of more than 24 hours and less than 120 hours; or

(c) unwelcome communications made at consistent and/or regular intervals

that have been confirmed by records available to your service provider.

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.

4.2.2 **What can you do?**

You should contact your service provider to ask what can be done to help stop the unwelcome communications.

You will need to explain to your service provider the nature of the unwelcome communications and the impact that these unwelcome communications are having on you.

Your service provider will inform you of the best solution for your circumstances. This may involve sending warning letters to the person from whom the unwelcome communications originate and/or referral to police.

If you are referred to the police, you may at this stage wish to request, as your preferred method of communication, a written acknowledgement from your service provider advising you have instigated the unwelcome communications process and present this to the police in your initial contact.

4.2.3 **Keeping records**

You will need to keep a record of the:

- times and dates of any unwelcome communications,
- calling number or other reference used to identify the service (e.g. email address) if known, or can be identified.

You must not delete records of the unwelcome communication(s) if you require assistance from your service provider and/or police.

Your service provider will need these details to assist in establishing a pattern of unwelcome communications that can be used as evidence of a pattern of unwelcome communications and to identify the supplier of service to the source of the unwelcome communications.

4.2.4 **Investigation and confirmation of a pattern of unwelcome communications**

Where evidence of a pattern of unwelcome communications is provided your service provider will commence an investigation to confirm the pattern of unwelcome communications.

4.2.5 **Service provider activity and limitations**

Where there is evidence of a pattern of unwelcome communications your service provider will undertake the following steps:

- Seek your consent in relation to your number or email address that received the unwelcome communications being disclosed to any other service provider that may be involved in the investigation as a supplier of services to the party that is initiating unwelcome communications and also to the person that originated the unwelcome communication.

- Seek your understanding that if you do not provide your consent to the disclosure of the number or email address that received the unwelcome communications, your service provider will be limited in the action it can take to assist you.

- Acknowledge that, subject to your consent being provided, where your service provider is also the service provider to the source of the unwelcome communications, the evidence of a pattern of unwelcome communications may be used as the basis for taking action to attempt to stop the unwelcome communications by sending a warning communication to the source of the unwelcome communications telling them to stop or further action will be taken.

- Acknowledge that, subject to your consent being provided where your service provider is not the same service provider as the source of the unwelcome communication, your service provider will send the information you have provided, together with any of its own data, to the service provider of the originating unwelcome communication. That service provider will be responsible for sending the warning communication to the originator of the unwelcome communications.

4.2.6 **Service provider limitations**

There are situations where your service provider having established that there is a pattern of unwelcome communications may be unable to assist, for example;

- following the issuing of a warning letter to cease the unwelcome communications (as per Clause 4.4.6 of the Code), there is an allowance of 10 business days to process the letter and for the source of the unwelcome communications to receive it. Your service provider is limited in the action they can take during this 10-business day period. During this time if you continue to receive unwelcome communications you should record the date and time for presentation to your service provider after the 10-business day period if required.

- where the identity of the originating unwelcome communications customer cannot be determined there is limited action that your service provider can take (as per Clause 4.4.13 of the Code). This could include a scenario where a perpetrator is Spoofing the CLI of a number. CLI spoofing can be a scenario where a false CLI has been injected into the A-Party communication.

- In the above case, you should see if the police can assist in resolving the issue (see Section 5 - Reporting to the police).

4.2.7 **Other actions you can take to limit the effect of unwelcome communications**

4.2.8 Your service provider can advise you of actions you can perform, to assist in possibly preventing further unwelcome communications – such as screening your communications, filtering your calls through an answering service such as voicemail, changing your number, etc.

4.2.9 You may notify the police at any stage during the investigation if at any time you fear for your life or safety and do not want to wait for the warning letter to be issued and delivered.

4.2.10 **If unwelcome communications continue after an initial warning has been sent**

If you continue to receive unwelcome communications after the 10-business day period allowed for the service provider to send the initial warning you should inform your service provider and provide them with the dates and times of the ongoing unwelcome communications.

At this point your service provider can arrange for a second letter to be sent stating that the unwelcome communications need to cease.

4.2.11 **If unwelcome communications continue after a second warning has been sent**

If you continue to receive unwelcome communications after 10 business days since the second warning has been sent you need to notify your service provider.

At this stage your service provider can arrange for suspension of the service used to send unwelcome communications.

Your service provider will inform you when the service used for originating unwelcome communications has been suspended.

4.2.12 **Reinstating a service associated with unwelcome communications**

The registered customer of the suspended service may guarantee in writing that the unwelcome communications will cease and in this case their service provider is able to reinstate the service. Your service provider will inform you if this happens.

4.2.13 **If unwelcome communications continue after reinstatement of a service**

If you continue to receive unwelcome communications within three years after the reinstatement of the service and your service provider is able to confirm that the unwelcome communications are originating from the same source your service provider can arrange for the originating service to be suspended or disconnected.

If you continue to receive unwelcome communications after the suspension or disconnection of the service your service provider will refer that your complaint to the police for possible resolution action.

4.2.14 **Closing an unwelcome communications case**

If there are no further unwelcome communications from the same originating source for three years your complaint case will be closed.

4.2.15 **If unwelcome communications start again after three years**

If unwelcome communications start again after three years, the warning letter process 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.

5 REPORTING TO THE POLICE

5.1 When you might consider taking the matter to the police

5.1.1 Life threatening or threat of serious harm

Where a telecommunications service has been used to threaten life or serious harm it may constitute a criminal offence under the Criminal Code Act 1995. For example, under section 474.15 of the Criminal Code Act 1995, it is a criminal offence if the communication is made to threaten to kill or to cause serious harm. These types of communications should be reported to the police immediately.

5.1.2 If you have received unwelcome communications

If you have been the victim of unwelcome communications, there are a range of matters that affect how the police may deal with the matter, and in some cases, unwelcome communications should not be raised with the police, as they may not be able to assist. (e.g. incorrect dialling or telemarketing. Refer to section 5.2).

5.1.3 When to seek police assistance

If you have a current order which prevents another party from communicating with you, then receiving a communication e.g. via a telephone call or SMS may breach the order and this will generally be dealt with as a breach of the order, not as an unwelcome communication and is a matter for the police in the first instance.

If you have received unwelcome communications through one or more communications channels (e.g. via phone call and SMS) from the same source that are menacing, harassing or offensive, note that this may constitute an offence. It is a criminal offence under the Criminal Code Act 1995 section 474.17 to make a communication in such a way that a reasonable person would regard it as being, in all the circumstances, menacing, harassing or offensive.

If either the A-Party customer cannot be identified or unwelcome communications continue after disconnection of the A-Party service, these types of communications may be reported to the police.

If referring unwelcome communications to the police in either of these cases, you should gain as much information as possible, in relation to the following:

- **Identity** – who is making the calls, including their name, address and other relevant information
- **Method** – how was the communication received e.g. telephone call, voicemail, SMS/MMS, etc.

- **Content** – what was the substance of the threat, menace, harassment, etc.?
- **When** – when did it occur and if more than once details of the events with dates and time
- **Evidence** – provide your account details including the name of your service provider / supplier and any phone records you may have such as evidence of received communications (e.g. telephone calls, SMS/MMS etc.) details of previous reports as unwelcome calls and details of any orders in existence (where applicable).

With such information police are able to seek further information from telecommunications service providers/suppliers under the criminal investigation release provisions to support a possible prosecution.

5.2 When police are unable to assist

Police are unable to assist in the following cases:

- **Incorrect dialling**

  Repeated communications from an incorrectly programmed fax service, message bank service or other technical service are not a police matter and should be reported to your service provider/supplier, not to police.

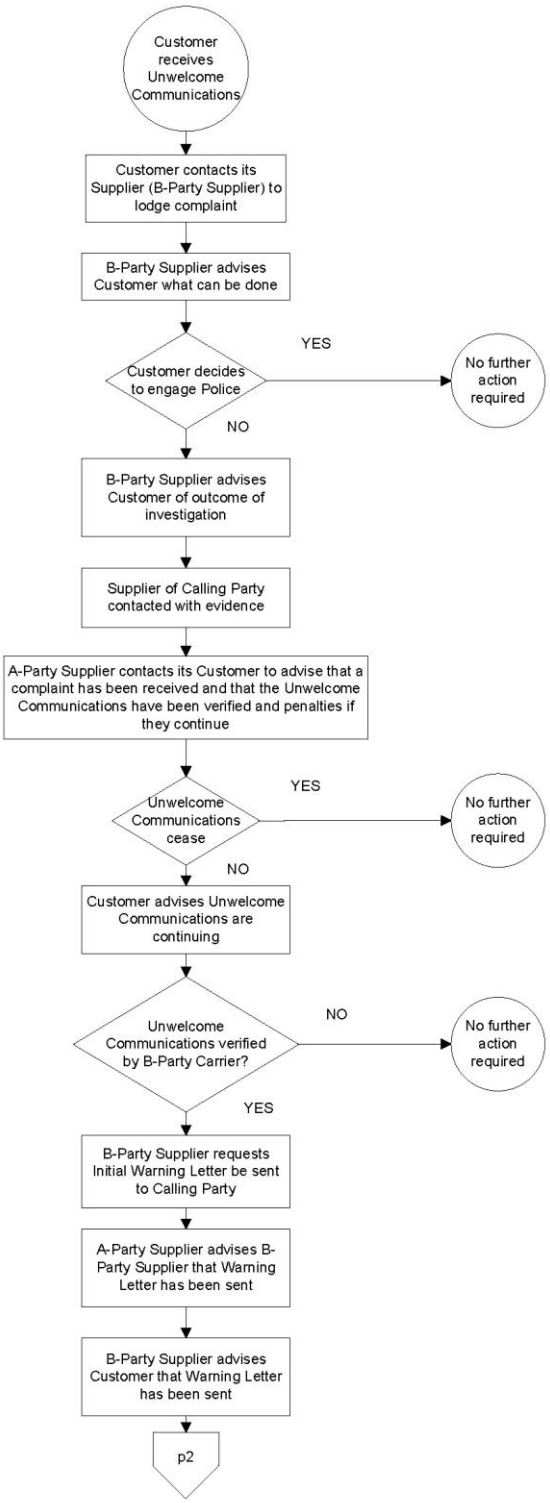
- **Telemarketing calls**

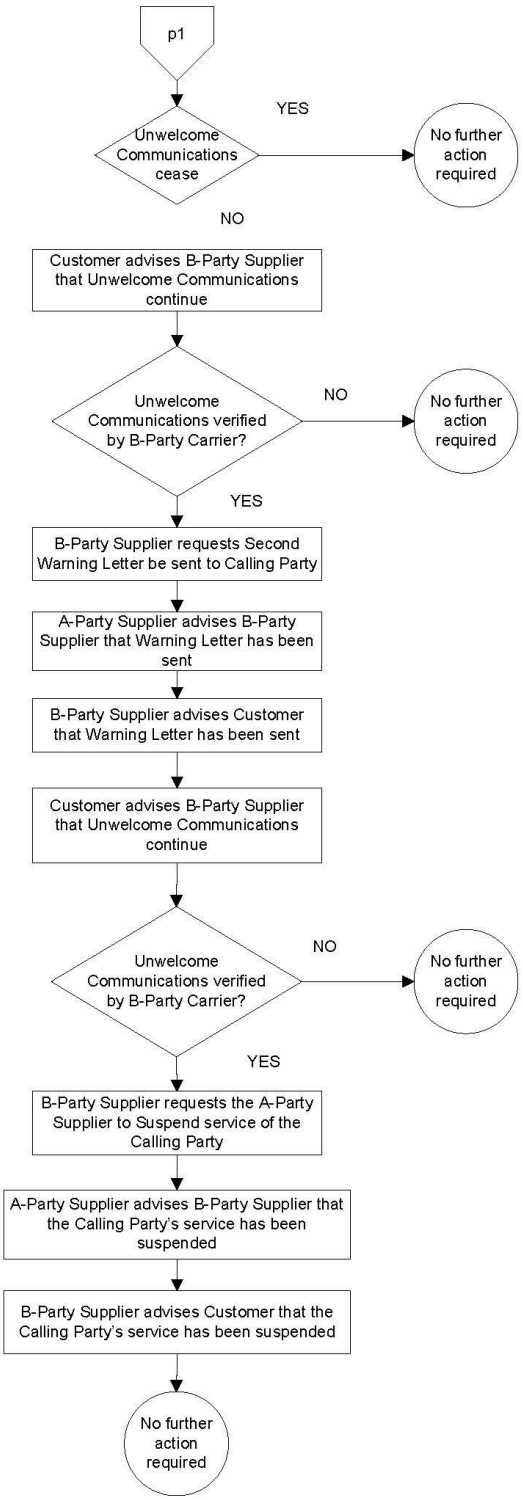
  If you are receiving telemarketing calls and no longer wish to do so, you should register your number with the Do Not call Register: https://www.donotcall.gov.au/

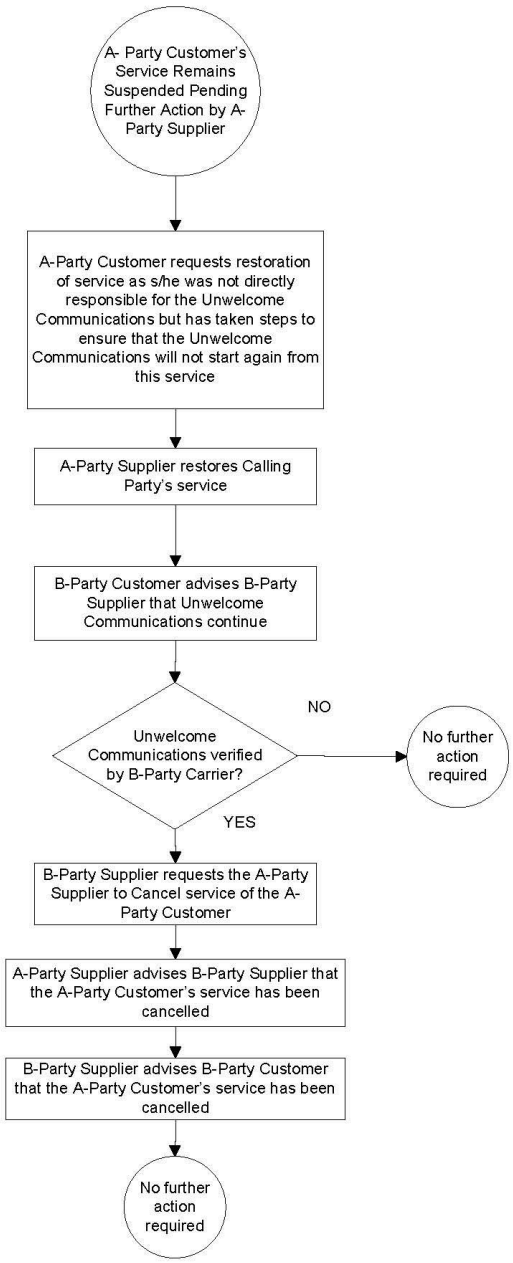
  If you are already registered with the Do Not call Register and still receiving telemarketing calls you can lodge a complaint with the ACMA: https://www.donotcall.gov.au/consumers/lodge-a-complaint/

APPENDIX

Customer Process Flow Charts




p1
Unwelcome Communications cease
YES
No further action required
NO
Customer advises B-Party Supplier that Unwelcome Communications continue
Unwelcome Communications verified by B-Party Carrier?
NO
No further action required
YES
B-Party Supplier requests Second Warning Letter be sent to Calling Party
A-Party Supplier advises B-Party Supplier that Warning Letter has been sent
B-Party Supplier advises Customer that Warning Letter has been sent
Customer advises B-Party Supplier that Unwelcome Communications continue
Unwelcome Communications verified by B-Party Carrier?
NO
No further action required
YES
B-Party Supplier requests the A-Party Supplier to Suspend service of the Calling Party
A-Party Supplier advises B-Party Supplier that the Calling Party's service has been suspended
B-Party Supplier advises Customer that the Calling Party's service has been suspended
No further action required



NOTE: If B-Party Customer receives no further Unwelcome Communications from the same service for 3 years, the Unwelcome Communications complaint is considered by the B-Party Supplier as closed.
If the B-Party Customer advises B-Party Supplier that the Unwelcome Communications have started again within the 3 year period and the B-Party Supplier is able to determine that the Unwelcome Communications have originated from the same service number as before, the B-Party Supplier will formally request that the A-Party Supplier SUSPEND or CANCEL the service. B-Party Supplier will advise the B-Party Customer that SUSPENSION or CANCELLATION has been requested. If Unwelcome Communications continue the B-Party Supplier will refer the B-Party Customer to Police for possible resolution.

Communications Alliance was formed in 1997 to provide a unified voice for the Australian communications industry and to lead it into the next generation of converging networks, technologies and services.

In pursuing its goals, Communications Alliance offers a forum for the industry to make coherent and constructive contributions to policy development and debate.

Communications Alliance seeks to facilitate open, effective and ethical competition between service providers while ensuring efficient, safe operation of networks, the provision of innovative services and the enhancement of consumer outcomes.

It is committed to the achievement of the policy objective of the *Telecommunications Act 1997* - the greatest practicable use of industry self-regulation without imposing undue financial and administrative burdens on industry.

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
TTY 61 2 9923 1911
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507