COMMUNICATIONS ALLIANCE LTD

INDUSTRY CODE

C661:2022

REDUCING SCAM CALLS and SCAM SMs

C661:2022 REDUCING SCAM CALLS and SCAM SMs Industry Code

First published as C661:2020

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

Disclaimers

1) Notwithstanding anything contained in this Industry Code:

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

      i) reliance on or compliance with this Industry Code;

      ii) inaccuracy or inappropriateness of this Industry Code; or

      iii) inconsistency of this Industry Code with any law; and

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

2) The above disclaimers will not apply to the extent they are inconsistent with any relevant legislation.

Copyright

INTRODUCTORY STATEMENT

Scams have severe social and financial impacts on users of telecommunications services in Australia. While vulnerable consumers are at the highest risk of being defrauded, even well informed and sophisticated consumers can fall victim when their telecommunications service is used to persistently deliver Scam Calls or Scam SMs, or in some cases their Number is used (spoofed) by scammers to make Scam Calls or send Scam SMs without their knowledge.

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

This Code sets out processes for identifying, tracing, blocking and otherwise disrupting Scam Calls and Scam SMs. The process is built on improved information sharing between Carriers/Carriage Service Providers (C/CSPs) as well as improved information sharing between industry and relevant government agencies. Communications Alliance (CA) and its members are committed to monitoring international best practice scam mitigation strategies in the context of the Australian environment as part of a continuous improvement model.

EXPLANATORY STATEMENT

This Explanatory Statement outlines the purpose of the Code and the public interest factors which have been taken into account at the time of the registration of the Code.

This Code replaces the C661:2020 **Reducing Scam Calls** Industry Code (the 2020 Code). Expressions used in this Explanatory Statement have the same meaning as in the Code.

Background

Scam activity on telco networks has a significant social and economic impact on Australians. The scale and effect of the activity is increasing. Scam activity is increasingly sophisticated and hard to detect. It usually originates offshore, readily adapts to disruption measures and ruthlessly exploits new opportunities and vulnerabilities.

Scammers perpetrate their crimes via a range of obfuscation techniques and scam types such as trying to steal money or identity through phone calls from live operators or robocalls.

Scams are a whole-of-community problem, and government, industry and consumers all have a role in mitigating associated detriments. CA wants to minimise Scam Calls and Scam SMs, reduce associated financial loss and hardship to customers and restore confidence in telecommunications networks.

Scammers are finding new ways to target Australian telephone customers. They are technologically adept, increasingly sophisticated and show no signs of stopping.

Current Regulatory Arrangements

On 2 December 2020, the Australian Communications and Media Authority (ACMA) registered the C661:2020 **Reducing Scam Calls Code** (the 2020 code) which was developed in response to the ACMA's Combating scams action plan that recommended the development of enforceable obligations on telcos to reduce Scam Calls.

How the Code Builds on and Enhances the Current Regulatory arrangements

The revised Code features improved tracing and reporting measures, along with a new section dealing with the identification, tracing, and blocking of numbers associated with Scam SMs.

The Code continues to provide a framework for co-operation and information-sharing among telecommunications service providers, that assists in the identification of scammers, so that blocking and enforcement action can more easily be taken.

What the Code will Accomplish

The Code will reduce Scam Calls and Scam SMs reaching customers. It provides clear requirements for telcos to work individually and collaboratively to combat Scam Calls and Scam SMs and protect customers from the associated harms. The Code recognises that empowered customers are a key defence against Scam Calls and Scam SMs by extending the obligations on telcos to provide information to assist their customers make more informed choices about the communications they receive.

How the Objectives will be Achieved

Scam activity will be disrupted by telcos working collaboratively, consistent with industry-agreed definitions and processes. Over 549 million Scam Calls were blocked in the first 16 months of operation of the 2020 code.

Anticipated Benefits to Consumers

The Code aims to reduce the number of Scam Calls and Scam SMs made by fraudsters and therefore stop these types of scams from making their way to consumers.

Consumers will benefit from piece of mind that they can trust the calls and SMs they are receiving, avoid the frustration of the intrusion of these scams and ultimately avoid the emotional and or financial impacts of falling victim to Scam Calls or Scam SMs.

Anticipated Benefits to Industry

The main benefit to the industry from the implementation of the Code will be a more uniform, collaborative and efficient approach to identifying, tracing and blocking Scam Calls and Scam SMs.

The Code allows for the automation of processes involved in the identification and tracing of Scam Calls and Scam SMs and the ability for C/CSPs to implement different solutions to combat scams.

Anticipated Cost to industry

There are costs associated with the establishment and maintenance of the support systems and bilateral agreements that will be needed to implement new provisions in the Code. Ongoing costs are likely to also be required to address the evolving ways in which fraudsters attempt to deceive consumers.

2022 Code Revision

This issue of the Code adds:

- obligations aimed at reducing Scam SMs, similar to the existing, and slightly updated, obligations which focus on reducing Scam Calls;
- obligations to notify the ACMA at various stages in the investigation and tracing process (for both Scam Calls and Scam SMs) to enable a holistic view of where combating scam traffic is at;
- the addition of an obligation to cancel services where an Australian Number is being used for 'call back' scams;
- templates for reporting on Scam Calls and Scam SMs to be provided to the ACMA; and
- editorial changes to improve clarity in the definitions and various sections of the Code.

John Laughlin
Chair
WC92 Reducing Scam Calls *Working Committee*

MAY 2022

TABLE OF CONTENTS

1 GENERAL

1.1 Introduction

1.1.1 Section 112 of the *Telecommunications Act 1997* (Cth) (Act) sets out the intention of the Commonwealth Parliament that bodies and associations representing sections of the telecommunications industry develop industry codes relating to the telecommunications activities of participants in those sections of the industry.

1.1.2 The development of the Code has been facilitated by CA through a Working Committee comprised of representatives from the telecommunications industry and ACMA.

1.1.3 The Code should be read in conjunction with CA G664:2022 and where the G664 Guideline sets out timeframes for actions, C/CSPs must adhere to these timeframes.

NOTE: G664:2022 is available for Industry participants only.

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

(a) the Act;

(b) the *Competition and Consumer Act 2010* (Cth);

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

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

(e) the *Privacy Act 1988* (Cth);

(f) the *Spam Act 2003 (*Cth*);*

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

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

(i) the Telecommunications (Interception and Access Regulations 2017; and

(j) the Telecommunications Numbering Plan 2015.

1.1.5 If there is a conflict between the requirements of the Code and any requirements imposed on a C/CSP by statute, the C/CSP will not be in breach of the Code by complying with the requirements of the statute.

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

1.1.7 Statements in boxed text are a guide to interpretation only and not binding as Code rules.

1.2 Registration by the ACMA

The Code is to be submitted to the ACMA for registration under section 117 of the Act.

1.3 Scope

1.3.1 The Code applies to the Carrier and CSP section of the telecommunications industry under section 110 of the Act.

1.3.2 The Code deals with the following telecommunications activities as defined in section 109 of the Act:

(a) carrying on business as a Carrier; or

(b) carrying on business activities as a CSP; or

(c) supplying goods or service(s) for use in connection with the supply or enablement of a Listed Carriage Service.

1.3.3 The Code applies to Scam Calls and Scam SMs that target customers. In complying with the Code, C/CSPs will have regard to the protection of communications provisions in the Act and the obligations at section 313 (1) of the Act and section 474.17 of the *Criminal Code Act 1995* (Cth).

1.3.4 The Code does not apply to matters covered by codes or standards registered or determined under the *Broadcasting Services Act 1992* (Cth) as required by section 116 of the Act.

1.3.5 The Code applies to Scam Calls and Scam SMs which are delivered via a Listed Carriage Service.

1.3.6 The Code does not apply to Scam Calls or Scam SMs that are delivered independently of a Carrier's or CSP's voice telephony switches or telecommunications messaging platforms (e.g. 'over the top' of a mobile data service).

1.3.7 The Code does not apply to calls made to an Emergency Call Person (ECP) or calls made from an ECP operator to an Emergency Service Organisation.

1.3.8 The Code requires C/CSPs to make best efforts to identify, trace, block and otherwise disrupt Scam Calls and Scam SMs.

1.4 Objective

1.4.1 The objective of the Code is to disrupt scam activity by:

(a) defining Scam Calls and Scam SMs in the context of the Code;

(b) establishing processes by which C/CSPs will work with each other and relevant government agencies to identify and reduce Scam Calls and Scam SMs;

(c) establishing processes to share and communicate evidence of Scam Calls and Scam SMs between C/CSPs and relevant government agencies;

(d) establishing processes for C/CSPs to exchange information in order to trace the origin of Scam Calls and Scam SMs;

(e) establishing a process for C/CSPs to Block Scam Calls and Scam SMs (from specific A-Party CLI(s));

(f) establishing a process to reinstate calls and SMs from Blocked A-Party CLI(s); and

(g) establishing a process for C/CSPs to restrict devices identified as originating Scam SMs from being used on a Carrier's network.

1.5 Code review

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

2 ACRONYMS, DEFINITIONS AND INTERPRETATION

2.1 Acronyms

For the purposes of the Code:

ACCC

means the Australian Competition and Consumer Commission.

ACMA

means the Australian Communications and Media Authority.

CA

means Communications Alliance.

C/CSP

means Carrier or Carriage Service Provider.

CDR

means Call Data Record.

CND

means Calling Number Display.

CLI

means Calling Line Identification.

CLIR

means Calling Line Identification Restriction.

CSP

means Carriage Service Provider.

ECP

means Emergency Call Person.

IMEI

means International Mobile Equipment Identity.

PABX

means Private Automatic Branch Exchange.

PEI

means Permanent Equipment Identifier.

PIN

means Personal Identification Number.

SM

means Short Message.

SMS

means Short Message Service.

URL

means Universal Resource Locator.

UTC

means Coordinated Universal Time.

XPOI

means across the point of interconnection between C/CSPs.

2.2 Definitions

For the purposes of the Code:

Act

means the *Telecommunications Act 1997* (Cth).

Alphanumeric Sender ID

means a personalised identifier (for example, the name of a business or organisation) instead of a Number.

Note: This is displayed on the B-Party's device for a received SM in lieu of the CLI.

A-Party

means the initiator of the call or SM.

Australian Number

means a Number allocated by the ACMA (e.g., numbers for use with a digital mobile service, geographic numbers, etc.).

B-Party

means the recipient of the call or SM.

Block

means to stop or otherwise disrupt the delivery of calls or SMs.

NOTE: Blocking can apply to incoming Scam Calls or Scam SMs to a Number, and outgoing Scam Calls or Scam SMs from a Number originating the Scam Calls or Scam SMs, or an Alphanumeric Sender ID associated with the Scam SMs.

Business Day

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

Calling Line Identification

means the data generated to identify the A-Party.

NOTE: The CLI may be generated by a Telecommunications Network, or it may be data generated outside of a Telecommunications Network to spoof a genuine Number.

Calling Number Display

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

Carriage Service

has the meaning given by section 7 of the Act.

NOTE: For the purposes of this Code, a Carriage Service means voice telephony or SMS 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.

NOTE: For the avoidance of doubt, a Carriage Service Provider includes an SMS aggregator.

Carrier

has the meaning given by section 7 of the Act.

CLI Restriction

has the meaning given by CA G500:2020.

CLI Spoofing

means the unauthorised use of a Number by an end user, where the A-Party is not the end user, and where the A-Party has injected a false CLI in an attempt to deliberately mask or mislead the B-Party about the identity of the originating caller or sender.

Emergency Call Person

has the meaning given by section 7 of the Act.

Emergency Service Organisation

has the meaning given by subsection 147(11) of the *Telecommunications (Consumer Protection and Service Standards) Act 1999* (Cth).

Inbound International Calls

means calls originating outside of Australia.

IMEI

has the meaning given in AS/CA S042.1:2022

International Operator

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

Listed Carriage Service

has the meaning given by section 16 of the Act.

Notifying C/CSP

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

Number

means a number specified in the Numbering Plan required by subsection 455(3) of the Act.

NOTE: This includes international numbers.

Numbering Plan

means the Telecommunications Numbering Plan 2015.

Originating C/CSP

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

PEI

has the meaning given in AS/CA S042.1:2022.

Rights of Use

has the meaning given by C566:2005 Rights of Use of Numbers or such other registered industry code that replaces C566:2005 Rights of Use of Numbers.

Scam Call

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

Scam SM

means any SM where:

a) the SM contains a link or a telephone number; and

b) the purpose, or apparent purpose, of the SM is to mislead or deceive a recipient of the SM into using the link or telephone number; and

c) the recipient would be likely to suffer detriment as a result of using the link or telephone number.

Short Message

has the meaning given by 3GPP Standard TS 23.040.

Short Message Service

means a messaging service to deliver SM to the B-Party using standardised communication protocols.

Telecommunications Network

has the meaning given by section 7 of the Act.

Terminating C/CSP

means a C/CSP that provides voice telephony services or SMS to a B-Party end user directly connected to the C/CSP.

Transit C/CSP

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

Unblock

means the reversal of a Block.

Universal Resource Locator

means a web resource that specifies its location on a computer network and a mechanism for retrieving it.

2.3 Interpretation

In the Code, unless the contrary appears:

(a) headings are for convenience only and do not affect interpretation;

(b) a reference to a statute, ordinance, code or other law includes regulations and other instruments under it and consolidations, amendments, re-enactments or replacements of any of them;

(c) words in the singular includes the plural and vice versa;

(d) words importing persons include a body whether corporate, politic or otherwise;

(e) where a word or phrase is defined, its other grammatical forms have a corresponding meaning;

(f) mentioning anything after include, includes or including does not limit what else might be included;

(g) words and expressions which are not defined have the meanings given to them in the Act; and

(h) a reference to a person includes a reference to the person's executors, administrators, successors, agents, assignees and novatees.

3 CONSUMER INFORMATION

3.1 Education information about Scam Calls and Scam SMs

3.1.1 C/CSPs must make available on their websites, up-to-date guidance material for customers which may include:

(a) the types of Scam Calls and Scam SMs related fraud risks to which customers may be exposed;

(b) information about products or services to assist in Blocking suspicious or unwanted Scam Calls and Scam SMs;

(c) the steps customers could take to mitigate those risks, such as:

(i) protecting their personal information and not sharing it with unknown or unsolicited callers;

(ii) contacting their financial institution immediately if they believe they have lost money to a scammer;

(iii) changing default PINs and passwords on newly acquired customer equipment;

(iv) selecting strong PINs and passwords (e.g. Not "1234" or "0000" or "password" etc.);

(v) locking devices with secure PINs;

(vi) ensuring that voicemail PINs are secure;

(vii) disabling PABX ports and features that are not used (e.g. remote call-forwarding);

(viii) changing PINs and passwords regularly;

(ix) not responding to missed calls or SMs from unknown international Numbers, unknown Australian Numbers or an unknown source;

(x) not clicking on URLs or making return calls to telephone Numbers contained in the SM from unknown international Numbers or unknown Australian Numbers or an unknown source;

(xi) Blocking suspicious or unknown Australian Numbers or international Numbers on devices and use of Blocking services or products, where available, on landlines; and

(xii) allowing unknown calls to go to voicemail and then listening to any message left to ascertain if this might be a genuine call.

(d) the actions that customers should take if they find that they have received Scam Calls or Scam SMs such as reporting the scam to www.Scamwatch.gov.au.

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

4 SCAM CALLS

4.1 Identifying Scam Calls

4.1.1 Scam Calls are often characterised by:

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

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

(b) Short duration;

(c) CLI issues:

(i) the A-Party CLI does not present to the Terminating C/CSP as a Number that can be called back, i.e. there is no way of verifying the originating A-party (for example the call cases where a dummy A-party CLI has been inserted by the Originating C/CSP for compliance with CA G549:2020 Interconnection Implementation Plan & CA G500:2020 Interconnect Signalling Specification);

(ii) the CND is Blocked with CLIR;

(iii) the A-Party CLI is from an 'incorrect' Number range, i.e. the Originating C/CSP has not been allocated the Number range, or the Number has not been ported to the Originating C/CSP;

(iv) the A-Party CLI of an Inbound International Call is an Australian Number (see CA G664:2022 for examples) or is not conforming to the ITU-T Recommendation E.164;

(v) the A-Party CLI is a Number which is longer than normal and/or is being generated from unallocated Number ranges;

(vi) the A-Party CLI is not used in accordance with the Numbering Plan; and

(vii) no A-Party CLI has been provided by the International Operator for an Inbound International Call.

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

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

(b) receiving customer complaints regarding phone calls that appear to be seeking information, for the purposes of committing fraud or where the customer has been scammed;

(c) customer complaints that their A-Party Number has been subject to CLI Spoofing;

(d) complaints to relevant government agencies about particular A-Party CLI being used for Scam Calls; and

(e) the CND details are invalid, or the Number presented as the A-Party CLI is valid but has been subject to CLI Spoofing.

4.2 Improving CLI accuracy

Domestically Originated Calls

4.2.1 Originating C/CSPs must prevent carriage of calls where the A-Party does not hold Rights of Use to the Number.

NOTE: Clause 4.2.1 does not impose any A-Party CLI accuracy validation requirements on Transit C/CSPs and Terminating C/CSPs for calls:

(a) *which are received XPOI from Originating C/CSPs or Transit C/CSPs;*

(b) *which are received via call redirection or call forwarding from a B-Party.*

4.2.2 C/CSPs must not send calls to International Operators without an A-Party CLI.

4.2.3 C/CSPs must not send calls to International Operators with a CLI which does not conform to the ITU-T Recommendation E.164 unless the CLI is associated with an international inbound mobile roaming service, or another format is agreed upon directly with the International Operator.

4.2.4 C/CSPs must not send calls to B-Parties on their own Telecommunications Network or XPOI to the Transit C/CSPs or Terminating C/CSPs where 13/1300/1800/1900 Australian Numbers are being used as A-Party CLI.

Internationally Originated Calls

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

NOTES: 1. See CA G549:2020 Interconnection Implementation Plan & CA G500:2020 Interconnect Signalling Specification for CLI compliance.
2. Where the A-Party CLI does not conform to the ITU-T Recommendation E.164, nor Recommendation ITU-T E.157 International Calling Party Number Delivery, then these calls should be subject to scrutiny as potential Scam Calls.
3. C/CSPs should not send Inbound International Calls to B-Parties on their own Telecommunications Network or XPOI to the Transit C/CSPs or Terminating C/CSPs where the A-Party CLI of an Inbound International Call is showing an Australian Number, unless exceptions apply (as per CA G664:2022).

4.2.6 C/CSPs must not send Inbound International Calls to B-Parties on their own Telecommunications Network or XPOI to the Transit C/CSPs or Terminating C/CSPs where the A-Party CLI of an Inbound International Call has not been provided by the International Operator.

Countering CLI Spoofing

4.2.7 If an Originating C/CSP identifies a material issue of alleged CLI Spoofing in calls from A-Parties, the Originating C/CSP must investigate and take action to stop the alleged CLI Spoofing.

4.2.8 Following the investigation and action taken in clause 4.2.7, if CLI Spoofing was confirmed, an Originating C/CSP must provide details about the CLI Spoofing (including where possible, the CLI of the A-Party) via agreed electronic means to the ACMA as per the template in Appendix B.

4.2.9 If a C/CSP identifies a material issue of alleged CLI Spoofing in calls received from other C/CSPs, that C/CSP (the Notifying C/CSP) must raise the issue, as soon as practicable, with the Originating C/CSP or the Transit C/CSP delivering the call traffic (with a copy to the ACMA), for investigation and action to stop the alleged CLI Spoofing.

4.2.10 If the Notifying C/CSP provides the notification under clause 4.2.9 to a Transit C/CSP, the Transit C/CSP must, as soon as practicable, forward the details, (with a copy to the ACMA) to the C/CSP from which they received those calls.

4.2.11 The process in clause 4.2.10 must be repeated by all Transit C/CSPs until the Originating C/CSP or International Operator is reached.

4.2.12 If CLI Spoofing is confirmed, the Originating C/CSP or adjacent Transit C/CSP must provide details about the CLI Spoofing (including, where possible, the CLI of the A-Party) via agreed electronic means to the ACMA as per the template in Appendix B.

4.2.13 If CLI Spoofing is found not to have occurred, the Originating C/CSP or Transit C/CSP must provide details about the calls to the adjacent Transit C/CSP or Notifying C/CSP, as soon as practicable, via agreed electronic means (with a copy to the ACMA).

4.2.14 The process in clause 4.2.13 must be repeated by all Transit C/CSPs until the Notifying C/CSP is reached.

4.3 Monitoring for Scam Calls

4.3.1 C/CSPs must monitor their networks for Scam Calls based upon;

(a) the characteristics in sections 4.1 and 4.2 noting that these characteristics are not intended to be exhaustive or restrictive in terms of monitoring that may occur; and

(b) the CLI notified by other C/CSPs or from relevant government agencies which are associated with potential Scam Calls.

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

4.4 Exchanging information about alleged Scam Calls

4.4.1 If a C/CSP identifies a material issue of alleged Scam Calls in calls received from other C/CSPs, that C/CSP (the Notifying C/CSP) must provide details of the alleged Scam Calls, to the Originating C/CSP or Transit C/CSP which delivered the alleged Scam Calls to it, for investigation as soon as practicable, via an agreed electronic means (with a copy to the ACMA).

4.4.2 Details of the alleged Scam Calls to be provided in a notification under clause 4.4.1 should be in the format set out in Appendix A and must include:

(a) the date and time (with UTC offset) of the alleged Scam Calls;

(b) the CLI used for the alleged Scam Calls;

(c) the number of alleged Scam Calls identified in the relevant period; and

(d) further evidence if requested by the Originating C/CSP or Transit C/CSP (e.g. customer complaints, call characteristics, CDRs) to support the identified calls as being alleged Scam Calls rather than legitimate calls.

4.4.3 C/CSPs must accept and acknowledge, via agreed electronic means (with a copy to the ACMA), receipt of a notification under clause 4.4.1.

4.4.4 If the Notifying C/CSP provides the notification under clause 4.4.1 to a Transit C/CSP, the Transit C/CSP must, as soon as practicable, forward the details (with a copy to the ACMA) to the C/CSP from which they received those calls.

4.4.5 The process in clause 4.4.4 must be repeated by all Transit C/CSPs until the Originating C/CSP or International Operator is reached.

4.4.6 If Scam Calls are confirmed, the Originating C/CSP or adjacent Transit C/CSP must provide details about the alleged Scam Calls (including, where possible, the CLI of the A-Party) to the ACMA, via agreed electronic means, as per the template in Appendix B.

4.4.7 If the alleged Scam Calls notified under clause 4.4.1 are found not to be Scam Calls, the Originating C/CSP or Transit C/CSP must provide details about the calls to the adjacent Transit C/CSPs and Notifying C/CSPs via agreed electronic means (with a copy to the ACMA).

4.5 Tracing Scam Calls

4.5.1 A C/CSP must have processes in place to trace the origin of alleged Scam Calls in accordance with section 4.4, whether the alleged Scam Calls originated on its own network or it was acting as a Transit C/CSP or Terminating C/CSP.

4.5.2 In accordance with the protection of communications provisions of the Act and the obligations at section 313(1) of the Act and section 474.17 of the *Criminal Code Act 1995* (Cth), C/CSPs must cooperate with each other in the prevention, investigation and mitigation of Scam Calls which are using their Carriage Services.

4.6 Blocking Scam Calls

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

4.6.2 Where Scam Calls are confirmed, each C/CSP in the transit path must:

(a) share information about the origin of the Scam Calls (including where possible the CLI of the A-Party) with the ACMA via agreed electronic means as per the template in Appendix B; and

(b) provide details about the transit path of the Scam Calls (including, where possible, the CLI of the A-Party) to relevant government agencies via agreed electronic means, as per the template in Appendix B.

4.6.3 Originating C/CSPs are responsible for investigating and undertaking appropriate action to Block the Scam Calls originating from their own directly connected A-Party customers. This should include the disconnection of the A-Party customer's service where Scam Calls are detected.

4.6.4 Where a C/CSP has formed a reasonable view that it has detected Scam Calls (based upon certain characteristics after considering section 4.1 and section 4.2), it may Block the Number associated with those Scam Calls.

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

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

4.6.6 Where an Originating C/CSP can identify the IMEI or PEI of the device being repeatedly used to send Scam Calls using different, or multiple Numbers, this may include restricting the use of the device by blocking the associated IMEI or PEI of that device across all mobile Carriers in Australia without prior warning.

4.7 Unblocking Numbers

4.7.1 Where a Number is found to be no longer being used for Scam Calls or was subject to CLI Spoofing, a C/CSP must take action to Unblock that Number as soon as practicable.

4.7.2 Where a Number is found to be incorrectly Blocked a C/CSP must take action to Unblock that Number as soon as practicable.

4.8 Seeking assistance from International Operators

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

4.9 Preventing use of Australian numbers for Scam

4.9.1 Where a C/CSP has formed a reasonable view that an Australian Number is being used to perpetrate (or attempt to perpetrate) a scam with the purpose of eliciting a response via either a voice callback or return SM, that C/CSP must notify the C/CSP that holds the Australian Number, as soon as practicable, of this reasonable view (and the evidence supporting the reasonable view).

4.9.2 The C/CSP that holds the Australian Number must investigate and if it determines the Australian Number is being used to perpetrate (or attempt to perpetrate) a scam it must:

(a) take action to prevent use of the Australian Number; and

(b) advise the ACMA details about use of the Number (including, where possible, the CLI of the A-Party) via agreed electronic means as per the template in Appendix B.

5 SCAM SMs

5.1 Identifying Scam SMs

5.1.1 Scam SMs are often characterised by:

(a) a high volume of messages to a large number of B-Parties;

(b) attempting to engage the consumer to click on a malicious URL;

(c) attempting to engage the consumer by eliciting a call or return SM to the scammer; and

(d) attempting to obtain personal information in order to impersonate the consumer.

NOTE: High volumes of SMs are not the primary evidence that the SMs originating from an individual Number are Scam SMs.

5.1.2 Scam SMs can also involve the misuse (impersonation) of the Alphanumeric Sender ID used by trusted brands (such as banks, telecommunications providers or government departments).

5.2 Improving Number and Alphanumeric Sender ID accuracy

5.2.1 Originating C/CSPs must prevent carriage of SMs where the A-Party does not hold Rights of Use to the Number.

NOTE: Clause 5.2.1 does not impose any A-Party CLI accuracy validation requirements on Transit C/CSPs and Terminating C/CSPs for SMs.

5.2.2 If a SM uses an Alphanumeric Sender ID, Originating C/CSPs must only originate SMs on their Telecommunications Network using an Alphanumeric Sender ID where:

a) it does not present as a Number; and

b) the Originating C/CSP has been provided evidence by the A-Party confirming that the A-Party has a valid use case for the Alphanumeric Sender ID.

NOTE: Clause 5.2.2 does not impose any Alphanumeric Sender ID accuracy validation requirements on Transit C/CSPs and Terminating C/CSPs for SMs which are:

a) received XPOI from Originating C/CSPs or Transit C/CSPs and/or International Operators; or

b) received via SM redirection or SM forwarding from a B-Party.

5.2.3 If a C/CSP identifies what it believes is a material misuse of an Alphanumeric Sender ID, that C/CSP (the Notifying C/CSP) must raise the issue, as soon as practicable, with the Originating C/CSP or the Transit C/CSP delivering the SMs (with a copy to the ACMA), for investigation and action to stop the alleged misuse of the Alphanumeric Sender ID.

5.2.4 If the Notifying C/CSP provides the notification under clause 5.2.3 to a Transit C/CSP, the Transit C/CSP must, as soon as practicable, forward the details, (with a copy to the ACMA) to the C/CSP from which they received those SMs.

5.2.5 The process in clause 5.2.4 must be repeated by all Transit C/CSPs until the Originating C/CSP is reached.

5.2.6 If Scam SMs are confirmed, the Originating C/CSP or adjacent Transit C/CSP must provide details about the alleged Scam SMs (including, where possible, the CLI of the A-Party) to the ACMA via agreed electronic means as per the template in Appendix C.

5.2.7 If the alleged Scam SMs using an Alphanumeric Sender ID notified under clause 5.2.3 are found not to be Scam SMs the Originating C/CSP or Transit C/CSP must provide details about the SMs to the adjacent Transit C/CSPs and Notifying C/CSPs, as soon as practicable, via agreed electronic means (with a copy to the ACMA).

5.3 Monitoring for Scam SMs

5.3.1 C/CSPs must monitor their networks for Scam SMs based upon;

(a) their characteristics in section 5.1 and 5.2, noting that these characteristics are not intended to be exhaustive or restrictive in terms of monitoring that may occur; and.

(b) the CLI notified by other C/CSPs or from relevant government agencies which are associated with informing of potential SMs.

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

5.4 Exchanging information about alleged Scam SMs

5.4.1 If a C/CSP identifies a material issue of alleged Scam SMs, that C/CSP (the Notifying C/CSP) must provide details of alleged Scam SMs, to the Originating C/CSP or Transit C/CSP delivering the alleged Scam SMs, for investigation as soon as practicable, via an agreed electronic means (with a copy to the ACMA).

5.4.2 Minimum details of the alleged Scam SMs to be provided to the Originating C/CSP or Transit C/CSP must include:

(a) the date and time (with UTC offset) of the alleged Scam SMs;

(b) the Number / Alphanumeric Sender ID used for the alleged Scam SMs;

(c) the number of alleged Scam SMs identified in the relevant period;

(d) further evidence if requested by the Originating C/CSP or Transit C/CSP (e.g., customer complaints, SMs characteristics, CDRs) to support the identified SMs as being alleged Scam SMs rather than legitimate SMs; and

(e) the content of the SMs, if available and disclosure is permitted under applicable legislation.

5.4.3 C/CSPs must accept and acknowledge, via an agreed electronic means (with a copy to the ACMA), receipt of a notification under clause 5.4.1 as soon as is practicable.

5.4.4 If the Notifying C/CSP provides the notification under clause 5.4.1 to a Transit C/CSP, the adjacent Transit C/CSP must, as soon as practicable, forward the details (with a copy to the ACMA), to the C/CSP from which they received those SMs.

5.4.5 The process in clause 5.4.4 must be repeated by all Transit C/CSPs until the Originating C/CSP is reached.

5.4.6 The Originating C/CSP must provide details about the alleged Scam SMs (including, where possible, the CLI of the A-Party) to the ACMA, via agreed electronic means as per the template in Appendix C.

5.5 Tracing Scam SMs

5.5.1 A C/CSP must have processes in place to trace the origin of alleged Scam SMs in accordance with section 5.4, whether the alleged Scam SMs originated on its own network or it was acting as a Transit C/CSP, or Terminating C/CSP.

5.5.2 In accordance with the protection of communications provisions of the Act and the obligations at section 313(1) of the Act and section 474.17 of *the Criminal Code Act 1995* (Cth), C/CSPs must cooperate with each other in the prevention, investigation and mitigation of Scam SMs which are using their Carriage Services.

5.5.3 When presented with evidence, under section 5.4 the Originating C/CSP must investigate and, where found to be Scam SMs, trace the origin of the Scam SMs as soon as practicable.

5.6 Blocking Scam SMs and restricting devices used to send Scam SMs

5.6.1 Originating C/CSPs are responsible for investigating and undertaking appropriate action to Block the Scam SMs originating from their own directly connected A-Party customers:

(a) Where an Originating C/CSP is the holder of the Number being used to send Scam SMs this should include the disconnection of the A-Party customer's service; or

(b) Where an Originating C/CSP can identify the IMEI or PEI of the device being repeatedly used to send Scam SMs using different, or multiple Numbers, this may include restricting the use of the device by blocking the associated IMEI or PEI of that device across all mobile Carriers in Australia without prior warning.

5.6.2 Where a C/CSP has formed a reasonable view that it has detected Scam SMs (based upon certain characteristics after considering section 5.1 and section 5.2), it may Block the Number associated with those Scam SMs.

5.7 Unblocking and removing restrictions on devices

5.7.1 Where a Number or Alphanumeric Sender ID is found to be no longer being used for originating Scam SMs or was subject to CLI Spoofing, a C/CSP must take action to Unblock that Number or Alphanumeric Sender ID as soon as is practicable.

5.7.2 Where a Number or Alphanumeric Sender ID is found to be incorrectly Blocked a C/CSP must take action to Unblock that Number or Alphanumeric Sender ID as soon as practicable.

5.8 Seeking assistance from International Operators

5.8.1 When a material number of Scam SMs are identified as originating internationally, C/CSPs must use all available contractual arrangements to secure the assistance of the relevant International Operator in stopping further Scam SMs into Australia.

6 REPORTING

6.1.1 C/CSPs must, within 20 Business Days of the end of each calendar quarter, report to the ACMA:

(a) For Scam Calls, in the format and detail specified in Appendix D; and

(b) For Scam SMs, in the format and detail specified in Appendix E.

7 C/CSP CONTACT LIST

7.1.1 For the purposes of meeting the information sharing and notification obligations under the Code, C/CSPs subject to the Code must register their contact details with CA.

7.1.2 C/CSPs must complete, maintain and keep their contact details up to date on an industry contact list and provide their details to CA within one Business Day for any new addition, or change to contact details.

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

Example contact list template

Carrier / CSP Name	Phone Contact	Email Contact	1st Level Escalation

8 REFERENCES

Publication	Title
Industry Documents	
C566:2005 Rights of Use of Numbers	
G549:2020 Interconnection Implementation Plan	
G500:2020 Interconnect Signalling Specification for Circuit Switched Networks	
G664:2022 Reducing Scam Calls and Scam SMs – Supplementary Information	
AS/CA S042.1:2022 -Requirements for connection to an air interface of a Telecommunications Network— Part 1: General.	
Recommendations	
ITU-T E.164 (11/2010)	
ITU-T E.157 (06/2021)	
3GPP Standard TS 23.040	
Legislation	
Criminal Code Act 1995	
Competition and Consumer Act 2010	
Do Not Call Register Act 2006	
Privacy Act 1988	
Spam Act 2003	
Telecommunications Act 1997	
Telecommunications (Consumer Protection and Service Standards) Act 1999	
Telecommunications (Emergency Call Service) Determination 2019	
Telecommunications Numbering Plan 2015	
Telecommunications (Interception and Access) Regulations 2017	

APPENDIX A

Sample for Scam Calls information sharing between C/CSPs

Details of Scam Call(s) (Refer to CA G664 Appendix A for a template to provide details)	*[Dates and times, duration, A-Party Number (associated CLI), number of Scam calls in the relevant period, and the relevant CDRs].*
Details of complaints received (if applicable)	*[number of complaints, reported loss, timing of complaints]*
Validation of CLI used for the Scam Call(s)	*[Type and nature of validation checks conducted, e.g., CLI callback, online search yielding evidence of complaints associated with CLI]* *[Outcomes of validation checks, e.g., CLI has been used to perpetrate illegitimate calls, CLI has been used legitimately for telemarketing calls, etc]*

Select from the following:

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

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

Contact Name: _____

Contact Number: _____

Signed: _____

Date: _____

APPENDIX B

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

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

Contact Name: _____

Contact Number: _____

Signed: _____

Date: _____

APPENDIX C

Sample for Scam SMs information sharing between C/CSPs

Details of Scam SMs	*[Dates and times, A-Party Number (associated CLI), number of Scam SMS in the relevant period, and the relevant CDRs].*
Details of complaints received (if applicable)	*[number of complaints, reported loss, timing of complaints]*
Validation of CLI used for the Scam SMs	

Select from the following:

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

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

Contact Name: _____

Contact Number: _____

Signed: _____

Date: _____

APPENDIX D

Sample for report for ACMA for Scam Calls blocked

Carrier/Carriage Service Provider (C/CSP) name:			
Contact person:			
Item	**Code Clause**	**Request for data**	
1	4.6.1	Number of scam calls blocked	
Breakdown of response to item 1 (above)			
1.1	4.2.1	Invalid or unallocated Australian numbers	
1.2	4.2.3	Invalid international numbers (unallocated country code or digit length <7 or >15)	
1.3	4.2.5	Australian fixed Calling Line Identification (CLI) from international source	
1.4	4.2.6	A-Party CLI of an Inbound International Call not provided	
1.5	4.2.4	13/1300/1800/1900 numbers	
1.6		Scam calls identified based on high volume, short duration characteristics at code clauses 4.1.1 and 4.1.2 (e.g., traffic likely to be Wangiri calls)	

APPENDIX E

Sample for report for ACMA for SMs blocked

Carrier/Carriage Service Provider (C/CSP) name:			
Contact person:			
Item	**Code Clause**	**Request for data**	
1	5.5.1	Number of SMs blocked	
Breakdown of response to item 1 (above)			
1.1	5.6.1 (a)	Blocked SMs originating from the C/CSPs own directly connected A-Party customers	
1.2	5.6.2	Blocked SMs received from Transit or Originating C/CSPs	

PARTICIPANTS

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

Organisation	Membership	Representative
Australian Communications and Media Authority (ACMA)	Non-voting	Bridget Smith
ACMA	Non-voting	John Mullaney
Australian Mobile Telecommunications Assoc. (AMTA)	Non-voting	Lisa Brown
Optus	Voting	Sanjeev Mangar
Optus	Non-voting	Warren Hudson
Optus	Non-voting	Jim Assarasakorn
Pivotel	Voting	Robert Sakker
Pivotel	Non-voting	Lachlan Highett
Sinch	Non-voting	Hugh Haley
Sinch	Voting	Luis Marques
Sinch	Non-voting	Brian Mullins
Symbio	Voting	Geoff Brann
Telstra	Voting	Tony Rayner
Telstra	Non-voting	John Laughlin
Telstra	Non-voting	Bob Spencer
TPG Telecom	Voting	Alexander R. Osborne
TPG Telecom	Non-voting	Annie Leahy
TPG Telecom	Non-voting	Mathew Wilson
TPG Telecom	Non-Voting	Neville Gabin
Twilio	Voting	Donald Connor
Twilio	Non-voting	Annemaree McDonough
Verizon Australia	Voting	Mary-Jane Salier
Vocus	Voting	Leanne O'Donnell
Vocus	Non-voting	Matthew Crippa

This Working Committee was chaired by John Laughlin of Telstra. Craig Purdon of Communications Alliance provided project management support.

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

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

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

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

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

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