Competition and Consumer Amendment (Scams Prevention Framework–Telecommunications Code) Instrument 2026

I, Anika Wells, Minister for Communications, as delegate of the Treasury Minister, make the following instrument.

Dated 2026

Anika Wells **[DRAFT ONLY—NOT FOR SIGNATURE]**
Minister for Communications

Contents

1 Name

This instrument is the *Competition and Consumer Amendment (Scams Prevention Framework—Telecommunications Code) Instrument 2026*.

2 Commencement

(1) Each provision of this instrument specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information		
Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. The whole of this instrument	The later of: (a) the start of the day after the day this instrument is registered; and (b) immediately after the commencement of the *Competition and Consumer (Scams Prevention Framework – Industry Codes) Instrument 2026*. However, the provisions do not commence at all if the event mentioned in paragraph (b) does not occur.	

Note: This table relates only to the provisions of this instrument as originally made. It will not be amended to deal with any later amendments of this instrument.

(2) Any information in column 3 of the table is not part of this instrument. Information may be inserted in this column, or information in it may be edited, in any published version of this instrument.

3 Authority

This instrument is made under section 58CB of the *Competition and Consumer Act 2010.*

4 Schedules

Each instrument that is specified in a Schedule to this instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to this instrument has effect according to its terms.

Schedule 1—Amendments

Competition and Consumer (Scams Prevention Framework – Industry Codes) Instrument 2026

1 After Schedule 1

Insert:

Schedule 2—Telecommunications Sector Code

Part 1—Preliminary

1 Title

This Code may be cited as the *Telecommunications Sector Code.*

2 Scope

This Code:

(a) is an SPF code made for covered telecommunications services which are designated as a regulated sector of the Australian economy; and

(b) applies to regulated entities for that regulated sector.

Note 1: A covered telecommunications service (within the meaning of the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026*) is either of the following services:

(a) a voice call service;

(b) a message service;

if the service is:

(c) provided by a carrier and a public carriage service provider (where the same person or different persons may act in the capacity of the carrier and the public carriage service provider); and

(d) provided using a listed carriage service.

For the designation of those services as a regulated sector, see section 13 of the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026.*

Note 2: A person who provides a covered telecommunications service is a regulated entity for that sector and that service is a regulated service of the regulated entity for the sector (see section 58AD of the *Competition and Consumer Act 2010*).

3 Interpretation

In this Code:

Act means the *Competition and Consumer Act 2010*.

assign has the same meaning as in C566:2023.

attach, to a voice call or message, means include signalling information or other information for transmission with the call or message over a telecommunications network.

Australian CLI, for a voice call, means a CLI that:

(a) identifies, or purports to identify, an Australian number; or

(b) otherwise indicates that the initiating party is using an Australian number to make the call.

Australian number has the same meaning as in the *Do Not Call Register Act 2006*.

authorised representative, in relation to a customer of a carrier or carriage service provider, means a person:

(a) who is listed by the customer on the customer's account as having authority from the customer to deal with the carrier or carriage service provider on behalf of that customer as the customer's representative; and

(b) whose personal information is recorded on the customer's account.

block means:

(a) in relation to a voice call or message – stop or otherwise disrupt the delivery of the call or message; or

(b) in relation to a CLI for a voice call – prevent the CLI for the call from being displayed to the receiving party.

business day means a day other than a Saturday, a Sunday or a public or bank holiday in the place concerned.

C566:2023 means:

(a) the Industry Code *C566:2023 Number management – Use of Numbers by Customers* first published in May 2023 by the company then known as Communications Alliance Ltd (now known as Australian Telecommunications Alliance Ltd) and registered by the ACMA under Part 6 of the *Telecommunications Act 1997*; or

(b) if:

(i) any other industry code is expressed to replace the industry code mentioned in paragraph (a); and

(ii) the replacement industry code is registered by the ACMA under Part 6 of the *Telecommunications Act 1997* –

the replacement industry code.

Note: A copy of C566:2023 could, at the time of making this Code, be obtained free of charge from:

(a) Australian Telecommunications Alliance Ltd's website at www.austelco.org.au; and

(b) the ACMA's the Register of industry codes kept under section 136 of the *Telecommunications Act 1997* which is made available on its website at www.acma.gov.au.

carriage service has the same meaning as in the *Telecommunications Act 1997.*

carriage service intermediary has the same meaning as in the *Telecommunications Act 1997.*

carriage service provider has the same meaning as in the *Telecommunications Act 1997.*

carrier has the same meaning as in the *Telecommunications Act 1997.*

CLI (short for calling line identification), for a voice call, is information that:

(a) is transmitted with the call over a telecommunications network; and

(b) identifies, or purports to identify, the number or other identifier associated with the carriage service used to make the call or the origin of the call; and

(c) may be displayed to the receiving party.

CLI spoofing means a CLI, for a voice call, that has been altered or fabricated, so as to display information that is misleading or unauthorised in relation to the carriage service used to make the call or the origin of the call.

covered telecommunications service has the same meaning as in the *Competition and Consumer (Scams Prevention Framework—Regulated Sectors) Designation 2026.*

Note: See Note 1 at the end of clause 2.

customer, in relation to a carrier or carriage service provider, means:

(a) a person (the ***person***) who has a contractual relationship with the carrier or carriage service provider for the supply of a covered telecommunications service; or

(b) an authorised representative of the person.

Do Not Originate List means a list established and maintained under subclause 18(2).

facility has the same meaning as in the *Telecommunications Act 1997.*

freephone number has the same meaning as in the Numbering Plan.

high-risk telecommunications service means:

(a) a service where the number associated with that service is neither allocated under the Numbering Plan nor assigned to the regulated entity providing that service; or

(b) a service for the carriage of inbound international voice calls to which an Australian CLI is attached; or

(c) a message aggregation service.

IMEI (short for International Mobile station Equipment Identity) has the same meaning as in AS/CA S042.1:2025.

inbound international message means a message originating outside of Australia and is, or is to be, carried into Australia for delivery.

inbound international voice call means a voice call originating outside of Australia and is, or is to be, carried into Australia for delivery.

initiating party, in relation to a voice call or message, is the party who makes the call or sends the message.

interconnected carrier or carriage service provider means a carrier or carriage service provider based in Australia that connects with, and passes traffic from, an international service provider or other international entity to any of the following in Australia:

(a) a transiting carrier or transiting carriage service provider;
(b) a terminating carrier or terminating carriage service provider;
(c) a receiving party who uses a covered telecommunications service supplied by the first-mentioned carriage service provider.

international CLI information, for a voice call, is CLI attached to the call and prepared by an international service provider.

international mobile roaming service has the same meaning as in:

(a) the *Telecommunications Service Provider (International Mobile Roaming) Determination 2019;* or
(b) if an instrument made under subsections 99(1) and 125AA(1) of the *Telecommunications Act 1997* replaces the instrument mentioned in paragraph (a) – the replacement instrument.

international service provider means an entity based outside of Australia who connects with, and passes traffic to, any of the following entities based in Australia:

(a) interconnected carrier or carriage service provider;
(b) a transiting carrier or transiting carriage service provider.

internet of things data-only number means a special services number that:

(a) has been specified for use in the Numbering Plan with an internet of things data-only service; and
(b) may only be used for that type of service.

internet of things data-only service has the same meaning as in the Numbering Plan.

interrupt, in relation to a voice call or message, means prevent the call or message from reaching the receiving party and can include:

(a) blocking the call or message; and
(b) redirecting the call or message to another place, such as a spam folder or answering service.

ITU-T Recommendation E.164 means ITU-T Recommendation E.164 – *The international public telecommunication numbering plan* first published in February 2026 by the International Telecommunication Union.

Note: A copy of ITU-T Recommendation E.164 could, at the time of making this Code, be obtained free of charge from ITU's website at www.itu.int.

legitimate use case:

(a) in relation to use of a telecommunications service by a person – means a case where it would be reasonable to conclude that the use of the telecommunications service by the person to make or receive voice calls or to send or receive messages:

(i) is for a legitimate purpose; and

(ii) would be unlikely to cause harm; and

(b) in relation to use of a trust marking — means a case where it would be reasonable to conclude that the use of the trust marking by the person for a voice call or message:

(i) is for a legitimate purpose; and

(ii) would be unlikely to cause harm.

listed carriage service has the same meaning as in the *Telecommunications Act 1997*.

local rate number has the same meaning as in the Numbering Plan.

message means a message (within the meaning of the *Spam Act 2003*) other than a message sent using a voice call service.

message aggregation service means a service supplied by a message aggregator.

message aggregator means a carriage service intermediary who uses its relationships with carriers to facilitate the sending of bulk messages, on behalf of other entities, through a single point of access.

message service means a service that enables messages to be sent or received using a carriage service (other than where a message is carried wholly over the internet).

mobile number has the same meaning as in the Numbering Plan.

network trust information means a marking or other information that is attached to voice a call or message to signal to other regulated entities that the call or message is legitimate.

no-verification signal, in relation to a voice call, means a marking or other information attached to the call to signal to other regulated entities that the call has not been verified as legitimate.

number means a number specified in the Numbering Plan in accordance with subsection 455(3) of the *Telecommunications Act 1997*.

Numbering Plan means:

(a) the *Telecommunications Numbering Plan 2025*; or

(b) if an instrument made under subsection 455(1) of the *Telecommunications Act 1997* replaces the instrument mentioned in paragraph (a) – the replacement instrument.

originating carriage service provider means a carriage service provider who:

(a) has a contractual relationship with a customer for the supply of a covered telecommunications service; and

(b) is responsible for enabling a voice call to be made or message to be sent by the initiating party who uses that service.

originating carrier means a carrier who:

(a) has a contractual relationship with a customer for the supply of a covered telecommunications service; and

(b) is responsible for enabling a voice call to be made or message to be sent by the initiating party who uses that service.

over-stamping means the replacement or modification of the original CLI, for a voice call, so as to display other information in relation to the carriage service used to make the call or the origin of the call.

PEI (short for Permanent Equipment Identifier) has the same meaning as in AS/CA S042.1:2025.

prepaid mobile carriage service has the same meaning as in:

(a) the *Telecommunications (Service Provider — Identity Checks for Prepaid Mobile Carriage Services) Determination 2017*; or

(b) if an instrument made under subsection 99(1) of the *Telecommunications Act 1997* replaces the instrument mentioned in paragraph (a) – the replacement instrument.

public carriage service provider means a carriage service provider (within the meaning of the *Telecommunications Act 1997*) other than a person who is a carriage service provider only because of subsection 87(3) of that Act.

public mobile telecommunications service has the same meaning as in the *Telecommunications Act 1997*.

receiving party, in relation to a voice call or message, is the party who receives, or is intended to receive, the call or message.

regulated entity means a regulated entity (within the meaning of the Act) for the regulated sector referred to in paragraph 2(a).

rights of use has the same meaning as in C566:2023.

rights-of-use check has the meaning given by clause 4.

scam traffic means traffic associated with scams.

sender identification has the same meaning as in the *Telecommunications Act 1997*.

SIP response code means a response code as set out in the SIP Interconnection Industry Guideline.

SIP Interconnection Industry Guideline means the Industry Guideline *G672:2023 Session Initiation Protocol (SIP) Interconnection* first published in

December 2023 by the company then known as Communications Alliance Ltd (now known as Australian Telecommunications Alliance Ltd).

Note: A copy of the SIP Interconnection Guideline could, at the time of making this Code, be obtained free of charge from Australian Telecommunications Alliance Ltd's website at www.austelco.org.au.

special services number has the same meaning as in the Numbering Plan.

SPF consumer means an SPF consumer (within the meaning of the Act) of a covered telecommunications service.

telecommunications network has the same meaning as in the *Telecommunications Act 1997.*

terminating carriage service provider means a carriage service provider who:

(a) has a contractual relationship with a customer for the supply of a covered telecommunications service; and

(b) is responsible for enabling a voice call or message to be delivered to the receiving party who uses that service.

terminating carrier means a carrier who:

(a) has a contractual relationship with a customer for the supply of a covered telecommunications service; and

(b) is responsible for enabling a voice call or message to be delivered to the receiving party who uses that service.

traffic means communications that are voice calls or messages passing over a telecommunications network.

transiting carriage service provider means a carriage service provider that connects with, and passes traffic between, any of the following:

(a) a carrier;

(b) a carriage service provider;

(c) an international service provider.

transiting carrier means a carrier that connects with, and passes traffic between, any of the following:

(a) a carrier;

(b) a carriage service provider;

(c) an international service provider.

trust marking means a marking or other information that is attached to a voice call or message to indicate to the receiving party that the call or message is legitimate.

voice call has the same meaning as in the *Do Not Call Register Act 2006*.

voice call service means a service that enables voice calls to be made or received using a carriage service (other than where a voice call is carried wholly over the internet).

Note: A number of other expressions used in this Code are defined in the Act, including the following:

(a) ACMA;
(b) actionable scam intelligence;
(c) regulated sector;
(d) regulated service;
(e) scam;
(f) SPF code;
(g) SPF personal information.

4 Meaning of rights-of-use check

In this Code, a ***rights-of-use check***, in relation to a number, is a check conducted by a regulated entity that verifies that a customer has rights of use in respect of the number by:

(a) confirming proof of association between the customer and the number; and
(b) demonstrating immediate access to the number by:
  (i) calling the number requiring immediate confirmation of a code provided to the customer; or
  (ii) sending a message with a unique verification code to the number, requiring immediate confirmation of the code; or
  (iii) sending a message with a unique URL to the number, requiring immediate activation.

5 References to other instruments

In this Code, unless the contrary intention appears:

(a) a reference to any other legislative instrument is a reference to that other legislative instrument as in force from time to time; and
(b) a reference to any other kind of instrument is a reference to that other instrument as in force from time to time.

Note 1: For references to Commonwealth Acts, see section 10 of the *Acts Interpretation Act 1901*; and see also subsection 13(1) of the *Legislation Act 2003* for the application of the *Acts Interpretation Act 1901* to legislative instruments.

Note 2: All Commonwealth Acts and legislative instruments are registered on the Federal Register of Legislation.

Note 3: For paragraph (b), see also subsection 58CC(4) of the Act.

Part 2—Telecommunications sector-specific obligations

Division A—Principle 2: prevent

6 Information about prospective and existing customers

(1) A regulated entity must, before entering into a contract with a person for the supply of a covered telecommunications service:

(a) verify the identity of the person; and
(b) if the service is a high-risk telecommunications service –

(i) verify that the person has the rights of use in respect of the number associated with the service, by conducting a rights-of-use check; and

(ii) establish a legitimate use case.

(2) A regulated entity must take reasonable steps to ensure that:

(a) the information the entity collects about each customer is accurate and up to date; and

(b) if the entity collects any further information about the customer for the purpose of correcting or updating the information the entity holds – the further information is also accurate and up to date.

7 No rights of use in respect of number

(1) This clause applies if a regulated entity is an originating carriage service provider.

(2) The regulated entity must prevent the carriage of a voice call or a message using any covered telecommunication service if the customer of the service does not have the rights of use in respect of the number associated with the service.

8 Obligation not to carry certain voice calls or messages

(1) A regulated entity must not, in supplying a covered telecommunications service, carry any voice call, unless a CLI for the call is attached.

(2) To avoid doubt, subclause (1) does not require a CLI for a voice call to be displayed to the receiving party.

Note: A CLI for a voice call can be blocked or over-stamped before reaching the receiving party in certain circumstances.

(3) A regulated entity must not, in supplying a covered telecommunications service, carry any inbound international voice call to which an Australian CLI is attached, unless:

(a) it is a case where:

(i) the CLI is associated with a mobile number; and

(ii) the entity has, in accordance with clause 9, determined that the call is legitimate; or

(b) it is a case where the entity may, in accordance with subclause 10(1), carry the call.

(4) A regulated entity must not, in supplying a covered telecommunications service, carry the following:

(a) any outbound voice call using a local rate number, freephone number or internet of things data-only number;

(b) any voice call or message using a number on any Do Not Originate List made available to the entity under subclause 18(4);

(c) any voice call or message to which network trust information is attached where that information is incorrect or incorrectly attached;

(d) any voice call or message to which a trust marking is attached if the marking is incorrect or incorrectly attached.

(5) A regulated entity must not, in supplying a covered telecommunications service, carry voice calls or messages to which a CLI is attached where the numbering format displayed is inconsistent with international standards, unless:

(a) the call is initiated using an international mobile roaming service; or

(b) the numbering format is one which an international service provider has agreed may be used.

Note: ITU-T Recommendation E.164 includes relevant international standards relating to the numbering format displayed for a CLI.

(6) A regulated entity must not, in supplying a covered telecommunications service, carry any inbound international voice call, unless a CLI for the call is attached and provided by the international service provider.

9 Inbound international voice call to which Australian CLI is attached that is associated with mobile number

(1) If a regulated entity:

(a) is an interconnected carrier or carriage service provider; and

(b) in supplying a covered telecommunications service, receives an inbound international voice call to which an Australian CLI is attached that is associated with a mobile number (the ***call***);

the entity must make a reasonable attempt to do one of the following to determine whether the call is legitimate:

(c) in a case where the entity may, in accordance with subclause 10(1), carry the call – verify the identity of the initiating party;

(d) verify that, at the time the entity receives the call:

(i) the mobile number is associated with the service; and

(ii) the service is being used to supply an international roaming service, activated by the customer;

(e) send the call to the carrier or carriage service provider who holds the number.

(2) If the regulated entity referred to in subclause (1) has made a reasonable attempt to do one of the things mentioned in that subclause but is unable to determine whether the call is legitimate, the entity must attach a no-verification signal to the call.

(3) If a regulated entity:

(a) is a terminating carrier or terminating carriage service provider; and

(b) in supplying the covered telecommunications service, receives a no-verification signal in relation to the call in accordance with subclause (2);

the entity must make a reasonable attempt to do one of the following to determine whether the call is legitimate:

(c) verify that, at the time the entity receives the call:

(i) the mobile number is associated with the service; and

(ii) the service is being used to supply an international roaming service, activated by the customer;

(d) send the call to the carrier or carriage service provider who holds the number.

(4) If the regulated entity referred to in subclause (3) has made a reasonable attempt to do one of things mentioned in that subclause but is unable to determine whether the call is legitimate, the entity must:
  (a) block the CLI for the call; or
  (b) before terminating the call, over-stamp the CLI for the call to indicate to the receiving party that the call originated outside of Australia and is unverified.

(5) To avoid doubt, a regulated entity may carry the call if the entity has, in accordance with this clause, determined that the call is legitimate.

10 Agreement for the carriage of inbound international voice calls

(1) A regulated entity may, in supplying a covered telecommunications service, carry an inbound international voice call to which an Australian CLI is attached (the ***call***) if:
  (a) a regulated entity who is an interconnected carrier or carriage service provider and a customer of that entity have entered into a written agreement that complies with subclause (2); and
  (b) the call is carried into Australia for delivery in a manner consistent with the agreement; and
  (c) the regulated entity who is a party to the agreement has:
    (i) verified the identity of the customer of that entity; and
    (ii) by conducting a rights-of-use check, verified that the customer has the rights of use in respect of the number associated with the service used to make the call.

(2) An agreement complies with this subclause if it specifies or otherwise deals with the following matters, relating to the use of Australian numbers for the carriage of inbound international voice calls:
  (a) the Australian numbers which may be used;
  (b) the reason that the customer wants to use the Australian numbers;
  (c) the persons who will send the calls to the regulated entity who is a party to the agreement;
  (d) the terms of use of the service supplied by the regulated entity under the agreement, including the arrangements and conditions for sending the calls.

11 International CLI information must be carried exactly as received

If a regulated entity, in supplying a covered telecommunications service, receives an inbound international voice call to which international CLI information is attached, the entity:
  (a) must not remove or alter any of that information; and
  (b) must carry that information exactly as received.

12 Customer's right to block all inbound voice calls and messages from numbers other than Australian numbers

(1) This clause applies if a regulated entity is a terminating carriage service provider.

(2) If, in relation to the supply of a covered telecommunications, a customer requests the regulated entity to block all inbound voice calls and messages from numbers other than Australian numbers, the entity must, as soon as practicable and within 5 business days after the day on which the request is made:
   (a) verify the identity of the customer; and
   (b) then, apply the block.

(3) The regulated entity must provide a simple means by which a customer may, easily and free of charge, request the application of a block of the kind referred to in subclause (2).

13 Trust marking

(1) A regulated entity must not, in supplying a covered telecommunications service, attach a trust marking to a voice call or message initiated using the service, unless the entity has:
   (a) verified the identity of the customer of the service; and
   (b) by conducting a rights-of-use check, verified that the customer has the rights of use in respect of the number associated with the service; and
   (c) established a legitimate use case.

(2) A regulated entity must take reasonable steps to ensure that its information technology systems and processes relating to trust markings are secure.

14 Network trust information

(1) If a regulated entity:
   (a) is an originating carriage service provider; and
   (b) is reasonably satisfied that a voice call or message initiated, using a covered telecommunications service, is legitimate;
   the entity must attach network trust information to the call or message before carrying the call or message.

(2) If a regulated entity:
   (a) is an interconnected carrier or carriage service provider; and
   (b) is reasonably satisfied that an inbound international voice call or inbound international message received, using a covered telecommunications service, is legitimate;
   the entity must attach network trust information to the call or message before carrying the call or message.

(3) A regulated entity must not, in supplying a covered telecommunications service, prevent the carriage of a voice call or message from another regulated entity who has correctly attached network trust information to the call or message, unless the call or message relates to an activity that has been investigated and is a scam.

(4) A regulated entity must take reasonable steps to ensure that its information technology systems and processes relating to network trust information are secure.

15 Preventing use of telecommunications infrastructure to commit scams

A regulated entity must, in connection with any telecommunications network or facility owned, operated or used by the entity for the supply of covered telecommunications services, take reasonable steps to implement secure systems and processes to prevent the network or facility from being used to commit scams.

16 Restrictions on sending messages using prepaid mobile carriage services

(1) This clause applies if a regulated entity is an originating carrier or originating carriage service provider in relation to a covered telecommunications service that is a prepaid mobile carriage service.

(2) The regulated entity must, before activating the prepaid mobile carriage service, impose a maximum limit on the volume of messages the customer may send, within a set period, to multiple numbers using the service.

(3) For the purposes of subclause (2), in imposing the maximum limit on the volume of messages and setting the period for that limit, the regulated entity must take into account the following:

(a) the volume or frequency of the messages that may be indicators of scam traffic;

(b) any history of previous scam traffic in relation to covered telecommunications services of the entity;

(c) typical legitimate use of prepaid mobile carriage services;

(d) the customer's characteristics;

(e) information received when verifying the identity of the customer.

Note: In relation to paragraph (d), for example, a customer who carries on a business may reasonably be expected to use the service to send a higher volume of messages to multiple numbers than a customer who uses the service principally for personal, household or domestic purposes.

17 Assistance to SPF consumer

(1) This clause applies if an SPF consumer:

(a) requests a regulated entity for assistance in relation to an activity that is or may be a scam in relation to a covered telecommunications service (***scam***); or

(b) indicates to the entity that the SPF consumer:

(i) is or may be a victim of a scam; or

(ii) has a higher risk of being targeted by a scam; or

(c) has been brought to the attention of the entity by a third party as someone who:

(i) is or may be a victim of a scam; or

(ii) has a higher risk of being targeted by a scam.

(2) The regulated entity must take reasonable steps to give assistance to the SPF consumer to help prevent and respond to scams, including by:

(a) identifying and activating appropriate and available telecommunications tools or service settings; and

(b) providing the SPF consumer with information that is clear, accessible and up to date about the following:

(i) common types of scams that may be received when using a covered telecommunications service;

(ii) practical steps that can be taken to identify and avoid scams;

(iii) action that should be taken if the SPF consumer identifies or suspects a scam;

(iv) how to report an activity that is or may be such a scam.

Note: In relation to paragraph (a), available telecommunications tools or service settings may include call or message blocking, call or message filtering, and controls relating to CLI or sender identification.

18 Do Not Originate List

(1) This clause applies if a regulated entity is an originating carrier or an originating carriage service provider.

(2) The regulated entity must establish and maintain a list of numbers, which are not used to make outbound voice calls or messages, to be known as the Do Not Originate List.

(3) The regulated entity must add a number to the Do Not Originate List when requested to do so by a customer of the entity, but only after the entity has:

(a) verified the identity of the customer; and

(b) by conducting a rights-of-use check, verified that the customer has the rights of use in respect of the number.

(4) The regulated entity must ensure that copies of the Do Not Originate List are made available to other regulated entities.

Division B—Principle 3: detect

19 Monitoring of telecommunications network and covered telecommunications service

(1) A regulated entity must actively monitor any telecommunications network, owned, operated or used by the entity to supply a covered telecommunications service, to detect any scams relating to, connected with, or using the service.

(2) Without limiting subclause (1), the regulated entity must take reasonable measures:

(a) for the real-time tracking of network activities to:

(i) validate the legitimacy of the traffic; and

(ii) identify any indicators of scam traffic; and

(b) for the analysis of information collected to identify:

(i) any actionable scam intelligence; and

(ii) any traffic patterns, trends, anomalies or other characteristics that may assist with the detection of any scams.

Note 1: The measures taken may involve the use various technologies, including advanced data analytics and predictive modelling.

Note 2: Indicators of scam traffic are characteristics of traffic that are commonly associated with scams and include, for example, one or more of the following:

(a) high-volume outbound voice calls or messages;

(b) CLI spoofing or unregistered sender IDs;

(c) geographic or routing irregularities.

(3) For the purposes of subclause (2), ***network activities*** are activities involving the carriage of traffic over a telecommunications network referred to in subclause (1).

20 Filtering of messages

(1) This clause applies if a regulated entity who is an originating carrier, originating carriage service provider or message aggregator.

(2) The regulated entity must use fully automated filtering technology for the detection of any scam material in messages carried by the entity using a covered telecommunications service.

(3) For the purposes of subclause (2), ***scam material*** is information that:

(a) has been used in an activity that is a scam; and

(b) is a mechanism or identifier of any of the following kinds:

(i) a number;

(ii) an email address;

(iii) a URL;

(iv) a hyperlink.

21 Giving notice of actionable scam intelligence

(1) This clause applies if a regulated entity:

(a) is a transiting carrier or terminating carriage service provider; and

(b) identifies or has actionable scam intelligence about an activity involving a voice call or message in relation to a covered telecommunications service of the entity.

Note 1: A regulated entity identifies or has actionable scam intelligence if (and when) there are reasonable grounds for the entity to suspect that the activity is a scam.

Note 2: A regulated entity may have intelligence that becomes actionable scam intelligence.

(2) The regulated entity must, as soon as practicable and within 5 business days after the relevant day, give written notice of the actionable scam intelligence to the following:

(a) if:

(i) the voice call or message originated in Australia; and

(ii) the originating carrier or originating carriage service provider is identifiable –

the originating carrier or originating carriage service provider;

(b) if:

(i) the call or message originated outside of Australia; and

(ii) the interconnected carrier or carriage service provider is identifiable –

the interconnected carrier or carriage service provider;

(c) if neither paragraph (a) nor paragraph (b) applies – the carrier or carriage service provider who connected with, and passed the traffic to, the regulated entity;

(d) if the carrier or carriage service provider who is required to be given notice under paragraph (a), (b) or (c) does not hold the number associated with the covered telecommunications service used to make the call or send the message – the carrier or carriage service provider who holds the number.

(3) For the purposes of subclause (2), ***relevant day*** is the day on which the regulated entity first identifies or has the actionable scam intelligence.

(4) The notice must contain any information that caused the regulated entity to suspect that the call or message is a scam.

(5) Any SPF personal information must be de-identified before it disclosed by way of the notice, unless the regulated entity reasonably believes that doing so would not achieve the object of Part IVF of the Act.

22 Acknowledging receipt of a notice of actionable scam intelligence

(1) This clause applies if a notice of actionable scam intelligence is given to a regulated entity (the ***first entity***) by another regulated entity (the ***second entity***) under subclause 21(2).

(2) The first entity must, as soon as practicable and within 2 business days after the day on which the notice is received, give the second entity written acknowledgement of receipt of the notice.

23 Informing regulated entity of outcome of investigation

(1) This clause applies if a regulated entity (the ***first entity***):

(a) is an originating carrier, originating carriage service provider or interconnected carrier or carriage service provider; and

(b) is given a notice by another regulated entity (***second entity***), under subclause (2) or otherwise, containing intelligence about an activity involving a voice call or message in relation to a covered telecommunications service, which becomes actionable scam intelligence for the first entity; and

(c) is required to take reasonable steps to investigate whether or not the call or message is a scam.

(2) The first entity must, as soon as practicable and within 2 business days after completing an investigation into whether or not the voice call or message is a scam, inform the second entity in writing of:

(a) the outcome of the investigation; and
(b) any relevant supporting information.

(3) Any SPF personal information must be de-identified before it is disclosed under subclause (2), unless the first entity reasonably believes that doing so would not achieve the object of Part IVF of the Act.

Division C—Principle 5: disrupt

24 Investigating actionable scam intelligence

(1) This clause applies if:
(a) a regulated entity has actionable scam intelligence about an activity involving a voice call or message in relation to a covered telecommunications service of the entity; and
(b) the entity must investigate whether or not the activity is a scam; and
(c) the intelligence identifies the number associated with the service used to make the call or send the message (the ***number***).

(2) If the regulated entity is a terminating carriage service provider, the entity must, while investigating whether or not the activity is a scam, take one of the following steps, before delivering any voice call or message from the number:
(a) in the case of a call – block the CLI for the call;
(b) in any case – attach a warning to the call or message.

(3) If the regulated entity is not a terminating carriage service provider, the entity must, while investigating whether or not the activity is a scam, take one of the following steps, before carrying any voice call or message from the number:
(a) in the case of a call – signal to any other regulated entity involved to block the CLI for the call;
(b) in any case – signal to any other regulated entity involved to attach a warning to the call or message.

(4) To avoid doubt, this clause does not limit the action that may be taken to disrupt:
(a) the activity; or
(b) any other activity that is the subject of actionable scam intelligence.

25 Scam activity

(1) This clause applies if:
(a) a regulated entity has intelligence about an activity involving a voice call or message in relation to a covered telecommunications service; and
(b) the intelligence identifies the number associated with the service used to make the call or send the message (the ***number***); and
(c) the activity has been investigated and is a scam.

(2) The regulated entity must, in supplying a covered telecommunications service, take reasonable steps to interrupt any voice call or message received from the number.

(3) If:

(a) the regulated entity is an originating carriage service provider; and
(b) there is a voice call or message from an SPF consumer to the number;

the entity must, before carrying the call or message, take reasonable steps to give the SPF consumer a warning.

(4) Subclauses (2) and (3) do not apply if the regulated entity reasonably believes that the number has been the subject of CLI spoofing.

(5) If:
(a) the regulated entity is an originating carriage service provider; and
(b) the intelligence referred to in subclause (1) identifies the IMEI or PEI of a device that was used in the scam activity; and
(c) the entity is aware that the IMEI or PEI of a device being used by a customer is the same as the IMEI or PEI of the device used in the scam activity;

the entity must make a reasonable attempt to interrupt the call or message.

26 Giving SIP response code or notice of interrupted voice call or message

(1) If a regulated entity interrupts a voice call or message (the ***action***) under subclause 25(2) or (4), the entity must do the following:
(a) return a SIP response code relevant to the action, unless it is not possible to do so;
(b) if it is not possible to return a SIP response code relevant to the action – promptly give a written notice of the action, including the reason for the action, to:
(i) if the originating carrier or originating carriage service provider is based in Australia – the originating carrier or the originating carriage service provider; or
(ii) if the originating carrier or originating carriage service provider is not based in Australia – the interconnected carrier or carriage service provider.

(2) For the purposes of subclause (1), it is not possible to return a SIP response code relevant to the action if that is due to:
(a) the operation or limitations of the Session Initiation Protocol; or
(b) constraints or failures of the underlying transport mechanisms; or
(c) other circumstances outside of the regulated entity's control.

27 Seeking assistance from international service providers

(1) This clause applies if:
(a) several voice calls or messages, using a covered telecommunications service, have been interrupted by a regulated entity; and
(b) the calls or messages originated outside of Australia; and
(c) the calls or messages were carried by the same international service provider to an interconnecting carrier or carriage service provider; and
(d) the regulated entity determines that the number of calls or messages is material.

(2) The regulated entity must use all available contractual arrangements to secure the assistance of international service providers in preventing the carriage of scam traffic to the interconnecting carrier or carriage service provider.

(3) For the purposes of paragraph (1)(d), the regulated entity must determine whether the number of voice calls or messages is material:

(a) using a risk-based approach; and

(b) taking into account to the following:

(i) the volume or frequency of the calls or messages;

(ii) the nature of scam traffic and the potential for such traffic to cause harm to SPF consumers;

(iii) the extent (if any) to which the calls or messages involve any misuse of Australian numbers;

(iv) any other relevant matter.

28 No scam activity

(1) This clause applies if:

(a) a regulated entity has intelligence about an activity involving a voice call or message in relation to a covered telecommunications service; and

(b) the intelligence identifies the number associated with the service used to make the call or send the message; and

(c) the activity has been investigated and is not a scam.

(2) The regulated entity must ensure that any action taken to disrupt the activity is promptly reversed, if it is reasonably practicable to reverse the action.

(3) Any reversal of action that is reasonably practicable must occur within 5 business days after the day on which the regulated entity becomes aware that the activity has been investigated and is not a scam.

29 Request to reverse any disruptive action

(1) This clause applies if:

(a) a regulated entity (the ***first entity***) has taken action to disrupt an activity involving a voice call or message in relation to a covered telecommunications service; and

(b) the first entity has received a request from another regulated entity (the ***second entity***) to reverse that action; and

(c) the request is accompanied by evidence that demonstrates that the activity is not a scam.

(2) The first entity must, as soon as practicable after receiving the request, give the second entity written acknowledgement of receipt of the request.

(3) If the first entity does not reverse the action within 2 business days after the day on which the request is received, the entity must give the second entity a written notice, including:

(a) the reasons for not reversing the action within the timeframe; and
(b) if:
(i) the first entity reasonably believes that the activity is not a scam; and
(ii) it is reasonably practicable to reverse the action –
the expected timeframe for reversal of the action which is consistent with subclause (4).

(4) Any reversal of action that is reasonably practicable must occur within 5 business days after the day on which the request is received.

Division D—Requirements to keep certain records

30 Verification of identity

(1) If a regulated entity verifies the identity of a person under this Code, the entity must keep a record of the verification method used by the entity.

(2) The record must be kept for at least 6 years after the day on which the identity of the person is verified.

31 Agreement referred to in clause 10

(1) If a regulated entity is an interconnected carrier or carriage service provider, who has entered into an agreement with a customer of the entity that complies with subclause 10(2), the entity must keep a copy of the agreement.

(2) The copy must be kept for at least 6 years after the day on which the agreement is made.

32 Security of SPF personal information contained in record

(1) This clause applies if a regulated entity is required to keep a record under this Code.

(2) The regulated entity must take reasonable steps to protect any SPF personal information contained in the record:
(a) from misuse, interference and loss; and
(b) from unauthorised access, modification or disclosure.

(3) The regulated entity must destroy or de-identify the SPF personal information as soon as practicable after the minimum retention period for the record, under this Code, has ended.

(4) Subclause (3) does not apply if the regulated entity is required by or under any other law to retain the SPF personal information.