New Zealand Telecommunications Forum

Code for Scam Calling and Scam SMS Prevention

("Scam Prevention Code")

Code Status:	Version 4 – Approved
Code Classification:	Voluntary Code
Date:	November 2022
Review Status:	Original version endorsed June 2018, V3 endorsed October 2019.

Introductory Statement

The New Zealand Telecommunications Forum Incorporated *Code for Scam Calling and Scam SMS Prevention ("TCF Scam Prevention Code")* is a code for Network Operators to agree on proactive steps to avoid and reduce, and reactive steps to identify, verify and take action on Scam Calls and Scam SMS to landlines and mobile phones.

Background

New Zealand, like many other countries, is targeted by scammers calling or texting national landline and mobile users. The scammers attempt to persuade anyone who answers their call, or receives their text, to cooperate in some way. Their objective is to extract funds from the recipient by deception, e.g., by tricking the victim into making a payment to the scammer or disclosing their credit card details.

This Code formalises a process and minimum standards between industry participants, to identify and block Scam Calling and Scam SMS activity, and to work proactively and collaboratively with the relevant external bodies to mitigate the risks to end users.

Anticipated benefits for Consumers

- Reduction in the number of Scam Calls and Scam SMS messages received by end users and the harm that can result from these.

Anticipated benefits for Industry

- A minimum consistent standard around prevention, identifying, verifying and blocking Scam Calls and Scam SMS.
- Reduction in the number of instances of Scam Calls and Scam SMS received by Network Operators.
- Minimise impact on legitimate traffic.

Language of the Code

This Code is intended to provide benefit for consumers; however, it is written to be read by industry experts rather than consumers, and this is reflected in the language and terminology used in the Code.

About the TCF

Established in 2002, the "New Zealand Telecommunications Forum" (TCF) is a registered incorporated society.

The TCF's objective is to actively foster cooperation among the telecommunications industry's participants, to enable the efficient provision of regulated and non-regulated Telecommunications Services. Our goal is to promote competition for the long-term benefit of end users of Telecommunications Services in New Zealand.

Code Structure

The Scam Prevention Code ("Code") consists of:

a) **This Code**, which sets out the scope, principles and requirements; and
b) The **Scam Calls/SMS Description List** – a list of known scams on the TCF website, that will be updated as new Scam Call and Scam SMS types are identified to support signatories and the public in achieving the purpose and objectives outlined in this Code.

Code Revision

1. A second iteration of this Code which corrects a wording error in Clause 9.14 of the initial version was issued in September 2018.
2. A third iteration of this Code which binds signatories to privacy law compliance was issued in October 2019.
3. This fourth iteration of the Code adds processes for managing Scam SMS and makes some minor amendments to the Scam Call processes to provide for scams involving number spoofing and call backs.

TABLE OF CONTENTS

A Defined Terms

A2P	Application to Person
A2P SMS Partner	means a party providing A2P SMS services either directly to business senders, or indirectly to business senders via an intermediary aggregator or aggregators, and who is directly connected to a mobile Network Operator.
Allowlist	means a mechanism where the default is that services are blocked, and services are individually allowed and opened up.
Billing Relationship	means a relationship where the Retail Service Provider has a bona fide right to charge the Customer for any chargeable activity relating to the provision of Telecommunications Services.
Blocking Traffic	means configuring the Network Operator, or A2P SMS Partner's voice switch or SMS switch or platform to stop a call or SMS from progressing with the intended consequence of failing the call or stopping the SMS. Blocking may be performed on specific number or numbers, shortcode or routes, or using content filters.
Business Day	means a day on which registered banks are open for normal banking business, excluding Saturdays, Sundays and nation-wide public holidays. Regional public holidays are considered to be Business Days.
CCF or Code Compliance Framework	means the TCF's Code Compliance Framework as endorsed by the TCF Board and being the overarching compliance and enforcement regime for TCF codes.
Clause	refers to a clause in this Code.
Code	means this Scam Prevention Code.
Code Signatory(s)	refers to a party that has signed up to this Code.
Compliance Officer	means the Person appointed by the TCF as the compliance officer under the Code Compliance Framework.
Customer	means a Person who has a bona fide Billing Relationship with a Retail Service Provider in respect of a Telecommunications Service.
Denylist	means a mechanism where the default is services being open, and services are blocked on an as-required basis.
Downstream Provider	means the Network Operator to whom a party directly sent an SMS or voice call.
Edge Network	means the Network Operator(s), having access to the New Zealand IPMS industry portability management system, closest to the source of the Scam Call or Scam SMS. Typically, these will be Network Operators with international connectivity, or domestic Network Operators where the scam originates within New Zealand.
Legitimate Call Notice	A notification to the TCF Scam Calls Notifications Distribution List in response to a Scam Call Advisory Notice or Verified Scam Call Notice to indicate that the traffic referred to is legitimate.
Legitimate SMS Notice	A notification in response to a Verified Scam SMS Notice to indicate that the individual SMS referred to is legitimate.
Network	means a system comprising telecommunications links to permit telecommunication.
Network Operator	means a network operator as that term is defined in section 5 of the Telecommunications Act 2001 that has a voice or SMS switch.

P2P	Person to Person
Person	means a legal person and includes a company and any other legal entity.
Relevant Provider	means a Network Operator or Service Provider who is relevant to a Scam SMS or Call who is not the Upstream Sender or Downstream Provider, for example in the case of where a Scam SMS encourages a voice call, the carrier to whom the number is ported in IPMS or TNAS (or who is the carrier of record where the number is not ported).
Retail Service Provider	means any Person providing a Telecommunication and/or Broadcast Service to a Customer and who has the Billing Relationship with the Customer for that service.
Scam Call(s)	means the use of voice telephony to gain by deception, typically involving mass inbound or outbound calling from, or to, unverifiable entities or known fraud entities which aim to steal money or information from recipients in New Zealand. Some examples of scam calling are fraudulent support calls and Wangiri (ring once and hang up) calls.
Scam Call Advisory Notice	A notification to the TCF Scam Calls Notifications Distribution List of activity that a Network Operator or Retail Service Provider reasonably suspects to be Scam Calls.
Scam Calls/SMS	means a Scam Call(s) or a Scam SMS(s) or a combination of both.
Scam Calls/SMS Description List	means the list of calling scams and SMS scams maintained by the TCF on their website under the heading Types of Scams, which explains the characteristics of phone scams and SMS scams. The List of Scam Calls and Scam SMS will be regularly updated on the TCF website as new scams are discovered.[1]
Scam SMS(s)	means the use of SMS to gain by deception, typically involving mass incoming messaging from unverifiable entities or known fraud entities which aim to steal money or information from recipients. Some examples of scam SMS are fraudulent information messages attempting to get the recipient to provide payment information such as credit card details via a weblink.
TCF	means the New Zealand Telecommunications Forum Incorporated.
TCF Scam Calls Notifications Distribution List	A private email distribution list, managed by the TCF, which Code Signatories can join in order to exchange information about Scam Calls according to the process in this Code.
TCF Scam SMS Notifications Distribution List	A private email distribution list, managed by the TCF, which Code Signatories can join in order to exchange information about Scam SMS according to the process in this Code.
Telecommunication(s) Service	means any good, service, equipment and/or facility that enables or facilitates Telecommunication.
Third Party	A third party who is permitted to send Third Party Notices and receive Verified Scam Call Notices and/or Verified Scam SMS Notices and is subject to an MoU with the TCF detailing this.
Third Party Notice	A notification of a reported scam to the TCF Scam Calls Notifications Distribution List or TCF Scam SMS Notifications Distribution List by a Third Party.
Un-Blocking Traffic	means removing any Blocking Traffic restrictions applied.
Upstream Sender	means the Network Operator from whom a party directly received an SMS or voice call.

[1] https://www.tcf.org.nz/consumers/digital-living/stay-safe-online/types-of-scams/

Verified Scam Call Notice	A notification to the TCF Scam Calls Notifications Distribution List of calls that are highly likely to be Scam Calls.
Verified Scam SMS Notice	A notification to the TCF Scam SMS Notification Distribution List or the Upstream Sender of SMS that are highly likely to be Scam SMS.
Wangiri	One ring and cut fraud, where the scammer hangs up after one ring or less, with the intention to entice the recipient to call the number back upon seeing a missed call. Refer to the SMS Calls/SMS Description List for further details.

B Introduction

1 Background

1.1 Scam Calls and Scam SMS are an increasingly common problem in New Zealand and internationally.

1.2 Some Network Operators and A2P SMS Partners in New Zealand have invested in a Scam prevention system to identify scams and/or have the capability to Block Traffic.

1.3 A common problem is use of A2P codes on a shared basis where scammers are able to use codes that look legitimate.

1.4 A newer issue is increasing prevalence of malware on end users' phones that sends malicious SMS without the end users' knowledge.

1.5 Both Scam Calls and Scam SMS have a high prevalence of having fake caller ID (e.g., phishing calls) or having caller ID that does not uniquely identify the caller/sender (e.g., missing or blank CLI on international voice calls, and "shared" A2P SMS short codes).

1.6 Organisations block scams for a variety of reasons including:

a) to protect end users, or

b) to protect their Networks

c) to prevent money flowing to scammers (e.g., for Wangiri calls) to reduce incentives for scammers.

1.7 Prior to the Code, Scam Calls were blocked by Network Operators on an informal and an ad-hoc basis between Network Operators with no systematic coordination for New Zealand Network Operator-wide blocking. The limited sharing of information contributed to opportunistic behaviour where Blocking Traffic by a Network Operator simply resulted in scammers sending that traffic via another Network Operator.

1.8 Building on the success of the process for Scam Calls, the Code has now been extended to include Scam SMS where A2P SMS Partners can work with Network Operators and Retail Service Providers to identify and stop Scam SMS.

1.9 Blocking Scam Calls/SMS and the flow-on reduction in money going to scammers will reduce the incentives for scammers to send Scam Calls/SMS to New Zealand and internationally.

2 Purpose

2.1 The purpose of this Code is to:

a) For services which are managed on a Denylist model (voice and P2P SMS), reduce the volume of Scam Calls/SMS by stopping them as close as possible to their source.

b) For services which are managed on an Allowlist model (A2P SMS), reduce the volume of Scam SMS by improving compliance with the Allowlist requirements.

c) Establish coordinated sharing of Scam Calls/SMS information in New Zealand and internationally to enable quicker responses and discourage Scam Calls through proactive and reactive controls.

d) Minimise the impact of inbound and outbound Scam Calls, and Scam SMS, on individual end users to reduce the risk of harm by making the public more aware of scams through the Scam Calls/SMS Description List.

e) Set out how Retail Service Providers, Network Operators and A2P SMS Partners identify and communicate Scam Calls/SMS between each other so they can act to ultimately stop the scams.

f) Educate end users so they can identify and respond appropriately to Scams Calls/SMS and provide a framework for the industry to identify new scams for inclusion on the Scam Calls/SMS Description List.

g) Provide a means for industry to share information with key stakeholders, including law enforcement agencies, on Scam Calls/SMS.

3 Objectives

3.1 The objectives of this Code are to:

3.1.1 Help protect New Zealand end users:

a) from financial scams resulting in monetary or other forms of loss.

b) by minimising the quantity of Scam Calls/SMS reaching New Zealand end users.

c) by maintaining end users' trust in voice and SMS Telecommunications Services.

d) by ensuring that end users feel safe from Scam Calls/SMS.

3.1.2 Facilitate the timely sharing between Operators of agreed Scam Calls/SMS information on the TCF Scam Calls Notifications Distribution List and the TCF Scam SMS Notifications Distribution List.

3.1.3 Agree consistent minimum standards on blocking of Scam Calls/SMS within New Zealand and internationally.

3.1.4 Specify a common process framework that Code Signatories will use to share information on Scam Calls/SMS while complying with privacy legislation and Code confidentiality obligations.

3.1.5 Govern the terms when Scam Calls/SMS information is shared. This common framework is crucial to providing a consistent approach to industry and end users.

3.1.6 To balance the above objectives with also minimising the impact on legitimate traffic.

4 Application

4.1 This Code applies to Retail Service Providers, Network Operators, and A2P SMS Partners that provide voice and/or SMS services to Customers.

5 Implementation

5.1 This Code was approved by the TCF Board on 10 November 2022.

5.2 This Code will take effect three months from the approval date.

6 Scope

6.1 This Code sets out the terms for sharing information between Retail Service Providers, Network Operators and A2P SMS Partners in New Zealand who are signatories to this Code, on potential Scam Calls and Scam SMS, that have been, or are blocked by a Network Operator or A2P SMS Partner on the basis prescribed within the Code.

6.2 This Code also covers the sharing of Scam Calls/SMS information for the purposes of investigating and blocking Scam Calls/SMS and/or the reporting of trends in scam calling and SMS for consumer education purposes, subject to compliance with Section 8.2.

6.3 Minimising impact of phishing and impersonation of legitimate numbers, by differentiating between legitimate and illegitimate traffic where possible, e.g., Un-Blocking Traffic initially blocked to protect against Scam Calls/SMS is an important part of the end user experience enabling a Network Operator to ensure legitimate traffic from legitimate numbers can resume.

6.4 For SMS, the scope of this Code includes A2P (Application to Person) SMS, and international P2P (Person to Person) SMS and domestic P2P SMS.

7 Exclusions from scope

7.1 This Code is not intended to cover or address:

7.1.1 Malicious or nuisance calls and SMS that do not meet the definition of a Scam Call/SMS.

7.1.2 Blocking of traffic that is not in compliance with other requirements e.g., valid caller ID, Allowlisting requirements for A2P SMS; or blocking of Network Operator or end user calls or SMS for other reasons such as non-payment.

7.1.3 The blocking of email or online messaging, for example WhatsApp, Messenger.

7.1.4 International revenue share fraud, which is covered by TCF's International Revenue Share Fraud Guidelines.

7.1.5 Inter-Network Operator Fraud.

7.2 Signatories need only comply with the sections of this Code which are relevant to their business, e.g., an A2P SMS Partner who does not have a calling business need not comply with the Scam Calling parts of this Code.

8 Principles

8.1 This Code will facilitate ongoing coordinated sharing of Scam Calls/SMS information between New Zealand Network Operators and other signatories or Third Parties and will be used to facilitate any new Network Operator into the sharing arrangement.

8.2 This Code is intended to agree a consistent minimum standard for end user protection committed to by signatories and does not preclude operators from having or agreeing bilateral arrangements providing a higher level of end user protection. In exercising their functions under this Code, Network Operators, Retail Service Providers and Third Parties sending Third Party Notices must:

8.2.1 comply with all relevant legislation, including the Privacy Act 2020, the Unsolicited Electronic Messages Act 2007 and the Telecommunications Act 2001; and

8.2.2 only use information shared by other parties pursuant to this Code for purposes directly related to and permitted by the Code.

C Managing Scams

9 Retail Service Providers

9.1 Retail Service Providers who receive information from Customers which the Retail Service Provider believes has the characteristics of a Scam Call/SMS will notify their Network Operator and/or A2P SMS Partner, and work with them to investigate if Customers are receiving Scam Calls/SMS.

9.2 Retail Service Providers will provide education information to Customers on their website warning Customers about scams and advising Customers where they can find additional information, and how to report Scam Calls/SMS. This must include information on how to report relevant Scam SMS to Te Tari Taiwhenua, Department of Internal Affairs (DIA).

10 Operational Requirements

10.1 Network Operators are responsible for how they detect Scams Calls/SMS on their own Network.

10.2 Network Operators, Edge Networks and A2P SMS Partners are responsible for how they Block Traffic on their Network but must do so in a way which balances protecting New Zealand end users from Scam Calls/SMS, with minimising the impact of blocking on legitimate traffic from legitimate numbers/users.

10.3 Network Operators must keep track of Customer reports of Scam Calls/SMS.

10.4 Network Operators, Retail Service Providers and A2P SMS Partners will advise the TCF of their generic Scam Calls Notifications email address and/or Scam SMS Notifications email address to be added to the TCF Scam Calls Notifications Distribution List and/or TCF Scam SMS Notifications Distribution List respectively, which are used to notify each other of potential and actual Scam Calls/SMS.

11 Managing Scam Calls

Sending a Scam Call Advisory Notice

11.1 If a Network Operator or Retail Service Provider detects activity that they reasonably suspect to be Scam Calls, they must send a Scam Call Advisory Notice to the Scam Calls Notification Distribution List.

11.2 The Scam Call Advisory Notice must include all of the following:

11.2.1 The telephone number(s) used for the call scam (the originating number for inbound scam calls, and the terminating number for outbound scam calls).

11.2.2 The characteristics of the scam.

11.2.3 Network traffic information and/or end user complaint information which supports the claim.

11.2.4 Identify the Upstream Sender and identify any other Relevant Provider, e.g. the owner of phone numbers presented as fake caller ID.

11.2.5 The subject line of the Scam Call Advisory Notice must include the words ‘Scam Call Advisory Notice’ followed by the telephone number used for the Scam Calls or the first number in the range if it is a range of numbers.

11.3 The sender of the Scam Call Advisory Notice may, at its own discretion, choose to Block Traffic identified on its Network relating to the Scam Call Advisory Notice. If the reporting Network Operator is an Edge Network, they must block the traffic.

Receiving a Scam Call Advisory Notice

11.4 When a Network Operator or Retail Service Provider receives a Scam Call Advisory Notice they should review the notice and consider whether they are seeing similar activity.

11.5 The recipient may choose, at its own discretion, to Block Traffic based on the information in the Scam Call Advisory Notice and/or take steps to address the scammer directly.

11.6 The recipient may inform other parts of its own business or relevant third-party business about the Scam Call Advisory Notice where they can take appropriate action to address the Scam Calls. These parties may share the Scam Call Advisory Notice with their Upstream Sender or (e.g. in the case of a call back to a number used in a Wangiri scam) Downstream Provider to reach the Edge Network who is best placed to take action.

11.7 If the recipient of a Scam Call Advisory Notice has additional information (e.g., consumer complaints) which can be used as evidence to indicate that the Scam Call Advisory Notice relates to a real Scam Call then they should send out a Verified Scam Call Notice to the Scam Calls Notification Distribution List as per Section 11.9.

11.8 Scam Call Advisory Notices do not need to be acknowledged by recipients.

Sending a Verified Scam Call Notice

11.9 If a Network Operator or Retail Service Provider detects activity that they reasonably suspect to be Scam Calls, or they receive notification via a Scam Call Advisory Notice, they can work directly with other Retail Service Providers and Network Operators to collate evidence to verify that the calls are Scam Calls.

11.10 Analysis of the calls is likely to require operators to share CDRs of examples of the calls between Network Operators to identify specific instances and understand call routing. CDRs contain private information and should only be shared between operators where there are appropriate privacy protections in place, and this is permitted for the purpose of identifying individual Scam Calls.

11.11 Where there is enough evidence to confirm that the calls are highly likely to be Scam Calls, a Network Operator must send a Verified Scam Call Notice to the Scam Calls Notification Distribution List.

11.12 The Verified Scam Call Notice must include all of the following:

11.12.1 The telephone number(s) used for the call scam (the originating number for inbound Scam Calls, and the terminating number for outbound Scam Calls).

11.12.2 The characteristics of the scam.

11.12.3 Network traffic information.

11.12.4 Complaint information gained from at least one end user on the nature of the calls which supports the claim. Note: personal information on the end users who provided the information should not be included in the Notice.

11.12.5 The Verified Scam Call Notice may also include Retail Service Provider(s) and/or Network Operator(s) involved in the investigation.

11.12.6 The subject line must include the phrase 'Verified Scam Call Notice' followed by the telephone number used for the Scam Calls or the first number in the range if it is a range of numbers.

Receiving a Verified Scam Call Notice

11.13 When a Network Operator or Retail Service Provider receives a Verified Scam Call Notice they may inform other parties of its own business or relevant third-party business about the Verified Scam Call Notice where they can take appropriate action to address the Scam Calls.

11.14 If the recipient is an Edge Network for the Scam Calls, then they must Block Traffic or otherwise stop the traffic based on the information in the Verified Scam Call Notice as soon as possible, and shall use reasonable efforts to do so within two hours.

11.15 The Edge Network should notify their Upstream Sender and any other Relevant Provider, that the Scam Calls have been blocked under this TCF Code.

11.16 Each Edge Network recipient should respond to the Scam Calls Notification Distribution List confirming they have Blocked Traffic within two hours of receipt of the Verified Scam Call Notice. The response to the Verified Scam Call Notice must include the following:

11.16.1 Date and time that blocking was actioned; and

11.16.2 Any other supporting/relevant notes.

11.16.3 The subject line must include the phrase 'Blocked Call Notice' followed by the telephone number used for the Scam Calls or the first number in the range if it is a range of numbers.

11.17 Calls should remain blocked for a minimum of four (4) weeks after the Verified Scam Call Notice has been received. After this time the calls can be un-blocked if the Scam Calls have stopped.

Legitimate Call Notice

11.18 If a Network Operator or Retail Service Provider receives a Scam Call Advisory Notice or a Verified Scam Call Notice which they believe is legitimate traffic they must send a Legitimate Call Notice to the Scam Calls Notification Distribution List.

11.19 The Legitimate Call Notice must include all of the following:

11.19.1 The telephone number(s) used for the calls (the originating number for inbound Scam Calls, and the terminating number for outbound Scam Calls).

11.19.2 Information which supports their claim that the calls are legitimate e.g., the name and type of business generating the calls.

11.19.3 The subject line must include the phrase 'Legitimate Call Notice' followed by the telephone number used in the original notice for the suspected Scam Calls or the first number if it is a range of numbers.

11.20 If a Network Operator receives a Legitimate Call Notice and is satisfied with the claim and supporting information that the Calls are legitimate and has Blocked Traffic, they should Un-Block Traffic if it does not breach other Network Operator requirements e.g., protection against nuisance calls under s112 of the Telecommunications Act.

Third Party Notice

11.21 A Third Party may be authorised to send Third Party Notices to Code Signatories in accordance with Section 16.

11.22 The Third Party Notice should include all the following information (where available):

11.22.1 The telephone number(s) used for the call scam (the originating number for inbound Scam Calls, and the terminating number for outbound Scam Calls)

11.22.2 The characteristics of the scam.

11.22.3 Network traffic information.

11.22.4 Complaint information gained from at least one end user on the nature of the calls which supports the claim. Note: personal information on the end users who provided the information should not be included in the Notice.

11.22.5 The organisation names of any Retail Service Provider(s) and/or Network

Operator(s) involved in the investigation.

11.22.6 The subject of the Third Party Notice must include the phrase 'Third Party Notice' followed by the telephone number used for the Scam Calls or the first number in the range if it is a range of numbers.

11.22.7 Contact information of the Third Party sending the notice.

12 Managing Scam Domestic P2P SMS

12.1 If a Network Operator or Retail Service Provider is notified by their Customer or by another Network Operator of a Scam SMS, or if they receive DIA reports on reported scams that identify the Network Operator's or Retail Service Provider's Customer as a sender of scam, they must investigate and take appropriate action. This may include:

12.1.1 Analysing the SMSs received by Customers to verify that the SMS are indeed scam issues, including reviewing the contents of the SMS message or messages and volumes of messages sent by the originating number. The Network Operator or Retail Service Provider shall identify the Network from which the SMS was sent.

SMS originated from another Network Operator's network

12.1.2 If there is enough evidence to confirm that the SMS are likely to be Scam SMS, the Network Operator shall follow their inter-operator process for such instances and report the scam to the relevant Upstream Sender for investigation and appropriate action, or ensure that the Upstream Sender has been advised by other means, e.g. via DIA reporting direct to the Upstream Sender as per the 7726 Scam reporting process.

SMS originated from Network Operator's own network

12.1.3 The Network Operator must investigate the source of the Scam SMS and, if they have the technical capability, assess whether scams were originated from a device of a legitimate Customer that was infected by a malware or from equipment used by a Customer in a fraudulent manner.

Where malware is assessed to be the sending mechanism, the Network Operator shall take appropriate action. This may include:

- Informing the Customer that suspicious activity was detected, advising on how to check their phone for malware and guiding the Customer towards instructions on how to remove it.
- If required, removing the affected Customer's ability to send SMS for a period of time, or until the Customer has taken certain action, in order to limit the impact on other users' or providers' operations or network.
- Taking other actions which seek to limit the impact on other users.

Where fraudulently used equipment, such as SIM boxes, is assessed to be the sending mechanism, the Network Operator shall take appropriate action. This may include:

- Permanently removing the Customer's ability to send SMS.
- Taking other actions which seek to prevent the scam from recurring, including reporting to Police to have the illicit equipment located and seized.
- Sharing information with other Mobile Network Operators.

12.2 The Network Operator or Retail Service Provider should encourage the Customer to notify DIA by sending details of the scam to 7726.

Third Party Notice

12.3 A Third Party may be authorised to send Third Party Notices to Code Signatories in accordance with Section 16.

12.4 The Third Party Notice should include all the following information (where available):

12.4.1 The telephone number(s) used for the Scam SMS

12.4.2 The characteristics of the scam.

12.4.3 Complaint information gained from at least one end user on the nature of the SMS which supports the claim. Note: personal information on the end users who provided the information should not be included in the Notice.

12.4.4 The organisation names of any Retail Service Provider(s) and/or Network Operator(s) involved.

12.4.5 The subject of the Third Party Notice must include the phrase 'Third Party Notice' followed by the telephone number used for the Scam SMS.

12.4.6 Contact information of the Third Party sending the notice.

13 Managing Scam International P2P SMS

Sending a Verified Scam SMS Notice

13.1 If a Network Operator detects activity for which there is enough evidence to confirm that the SMS are highly likely to be Scam SMS, they should send a Verified Scam SMS Notice to the Upstream Sender, or ensure that the Upstream Sender has been advised by other means, e.g. via DIA reporting direct to the Upstream Sender as per the 7726 Scam reporting process.

13.2 The Verified Scam SMS Notice should include all of the following:

13.2.1 The contents of the SMS message or messages.

13.2.2 The originating number or numbers, and if possible, example b-numbers and relevant time/date details.

13.2.3 The Notice may also include additional information, for example the detected volume of messages.

13.3 Network Operator should take steps to limit the risk to their Customers from fraud. This may include for example blocking of URLs or outbound telephone numbers used in the fraud or notifying the carrier of record for the phone number, if the Scam SMS contains actionable content (such as a URL to click or a phone number to reply).

Receiving a Verified Scam SMS Notice

13.4 When the Upstream Sender receives a Verified Scam SMS Notice they shall take appropriate action. This may include:

13.4.1 Reporting the scam to the relevant Customer or Upstream Sender for investigation and appropriate action to address the Scam SMS.

13.4.2 If they have the technical capability, blocking the sender of the traffic on their platform.

13.4.3 as far as possible, identifying the source of the Scam SMS and taking action to prevent the scam from recurring.

13.5 If blocking action is taken, the Upstream Sender must inform the affected Network Operator or Network Operators that it has blocked the sender by replying to the relevant Verified Scam SMS

Notice to the Scam SMS Notification Distribution List, with the subject line unchanged.

Sending a Legitimate SMS Notice – Upstream Sender

13.6 If the Upstream Sender receives a Verified Scam SMS Notice for which they believe the individual SMS complained about is legitimate traffic, they must send a Legitimate SMS Notice to the Network Operator.

13.7 The Legitimate SMS Notice must include all the following:

13.7.1 The number or numbers used for suspected scam notice.

13.7.2 Information which supports their claim that the individual SMS complained about is legitimate e.g., the name and type of business and business purpose for the message sent.

13.7.3 The subject line must include the phrase 'Legitimate SMS Notice' followed by the number or numbers used in the original notice for the Verified Scam SMS Notice.

13.8 If a Network Operator receives a Legitimate SMS Notice and is satisfied with the claim and supporting information that the SMS complained about are legitimate, and has Blocked Traffic they should Un-Block Traffic, if the traffic does not breach other Network Operator requirements.

Third Party Notice

13.9 A Third Party may be authorised to send Third Party Notices to Code Signatories in accordance with Section 16.

13.10 The Third Party Notice should include all the following information (where available):

13.10.1 The telephone number(s) used for the Scam SMS

13.10.2 The characteristics of the scam.

13.10.3 Complaint information gained from at least one end user on the nature of the SMS which supports the claim. Note: personal information on the end users who provided the information should not be included in the Notice.

13.10.4 The organisation names of any Retail Service Provider(s) and/or Network Operator(s) involved.

13.10.5 The subject of the Third Party Notice must include the phrase 'Third Party Notice' followed by the telephone number used for the Scam SMS.

13.10.6 Contact information of the Third Party sending the notice.

Information Sharing

13.11 Network Operators should on regular basis share information with other Network Operators, TCF and DIA regarding trends, learnings around actions taken and any other relevant information that could reduce risk to mobile users.

14 Managing Scam A2P SMS

Sending a Verified Scam SMS Notice

14.1 If a Network Operator or Retail Service Provider or A2P SMS Partner detects activity that they reasonably suspect to be Scam SMS they must send a Scam SMS Verified Notice to the Scam SMS Notification Distribution List.

14.2 The Scam SMS Advisory Notice should include all of the following:

14.2.1 The contents of the SMS message or messages, pasted into the SMS Advisory Notice as an image (e.g., screenshots of content message and any URLs).

14.2.2 The originating short code that has been transmitted out to each Network Operator, and if possible, example b-numbers and relevant time/date details.

14.2.3 The subject line of the Verified Scam SMS Notice must include the words 'Verified Scam SMS Notice' followed by the short code used for the Scam SMS

14.2.4 The Notice may also include additional information, for example the detected volume of messages.

Receiving a Verified Scam SMS Notice – Originating A2P SMS Partner

14.3 When the A2P SMS Partner who originated the Scam SMS as identified by the short code used by the scammer receives (or sends) a Verified Scam SMS Notice they must:

14.3.1 Block the traffic on their platform as soon as possible, and shall use reasonable efforts to do so within two hours.

14.3.2 As far as possible, identify the source of the Scam SMS and take action to prevent the scam from recurring (e.g., take action to prevent the traffic shifting to use a different short code or short codes).

Receiving a Verified Scam SMS Notice – Network Operator

14.4 When a Network Operator receives a Verified Scam SMS Notice they must:

14.4.1 If they have the technical capability block the sender of the traffic on their platform.

14.4.2 As far as possible, identify the source of the Scam SMS and take action to prevent the scam from recurring (e.g., work with the relevant A2P SMS Partner, to understand what other short codes are used by the same aggregator, and take action to prevent the traffic shifting to use a different short code or short codes).

14.5 A Network Operator must inform the affected A2P SMS Partners that is has blocked the sender (short code) by replying to the relevant Verified Scam SMS Notice to the Scam SMS Notification Distribution List, with the subject line unchanged.

14.5.1 The reply to the Verified Scam SMS Notice should include details of:

a) When the block was put in place.

b) The expected duration of the block.

c) The volume of messages sent before the activity was blocked.

d) Any other actions the Network Operator has taken relating to the scam.

Proactive Blocking of Traffic by A2P SMS Partners

14.6 If an A2P SMS Partner confirms suspicious activity or suspicious content to be phishing or scam, they must immediately Block the traffic and send a Verified Scam SMS Notice to the Scam SMS Notification Distribution List.

14.7 The Scam SMS Advisory Notice must include all of the following:

14.7.1 The contents of the SMS campaign, pasted into the Notice as an image (e.g., screenshots of content message and any URLs).

14.7.2 The originated short code/s or number/s that was used (or was attempting to be used).

14.7.3 Where some Scam SMS were sent before the content was blocked, the volume of

messages sent before the activity was blocked.

14.8 The subject line of the Verified Scam SMS Notice must include the words 'Advisory (Blocked) Scam SMS Notice' followed by the short code used for the Scam SMS.

Sending a Legitimate SMS Notice – the Originating A2P SMS Partner

14.9 If the Originating A2P SMS Partner receives a Verified Scam SMS Notice for which they believe there has been an error e.g., the wrong short code has been reported in the notice, or the individual SMS complained about did not originate from them, or that the report is maliciously false, i.e., that their traffic is legitimate traffic, they must send a Legitimate SMS Notice.

14.10 The Legitimate SMS Notice must include all of the following:

14.10.1 The SMS Short code used for suspected scam notice.

14.10.2 Information which supports their claim that the individual SMS complained about are legitimate e.g., the name and type of business generating the messages.

14.10.3 The subject line must include the phrase 'Legitimate SMS Notice' followed by the SMS short code used in the original notice for the Verified Scam SMS Notice.

14.11 If a Network Operator receives a Legitimate SMS Notice and is satisfied with the claim and supporting information that the SMS complained about are legitimate, and has Blocked Traffic they should Un-Block Traffic, if the traffic does not breach other Network Operator requirements.

Third Party Notice

14.12 A Third Party may be authorised to send Third Party Notices to Code Signatories in accordance with Section 16.

14.13 The Third Party Notice should include all the following information (where available):

14.13.1 The shortcode(s) used for the Scam SMS

14.13.2 The characteristics of the scam.

14.13.3 Complaint information gained from at least one end user on the nature of the SMS which supports the claim. Note: personal information on the end users who provided the information should not be included in the Notice.

14.13.4 The organisation names of any Retail Service Provider(s) and/or Network Operator(s) involved.

14.13.5 The subject of the Third Party Notice must include the phrase 'Third Party Notice' followed by the telephone number used for the Scam SMS.

14.13.6 Contact information of the Third Party sending the notice.

15 Information from DIA

15.1 Code Signatories are encouraged to engage directly with DIA to receive regular updates on reported scams, and to use this information as part of their scam mitigation processes. Information on engaging with the DIA can be provided by the TCF. You can also contact the DIA Digital messaging team at info@antispam.govt.nz.

16 Third Party Engagement

16.1 The TCF may permit Third Parties (e.g., government agencies, online safety organisations) to receive Verified Scam Call Notices and/or Verified Scam SMS Notices sent between Code

Signatories and/or send Third Party Notices where these support the Purpose and Objectives of this Code, as outlined in section B.

16.2 Third Parties who wish to receive and/or send Notices should request access via the TCF CEO stating how they propose to engage with the process and the benefits this would provide to end users.

16.3 The TCF CEO will seek the agreement of Code Signatories before approving a Third Party's access.

16.4 A MoU between the TCF and the Third Party will be used to detail the level of access given and the Third Party's obligations.

16.5 The TCF will reserve the right to terminate a Third Party's engagement with the process where it is adversely impacting the operation of the Code or for any other reason.

16.6 The TCF shall review the list of Third Parties who receive and/or send Notices on an annual basis to confirm their continued engagement is beneficial to the Purpose and Objectives of this Code.

D Scam Calls/SMS Description

17 Scam Calls/SMS Description List

17.1 The TCF will publish consumer-friendly information about known scams on its website in the form of a Scam Calls/SMS Description List.

17.2 The TCF Scam Calls/SMS Description List will include the description of the scam and its key characteristics.

17.3 The TCF will regularly update the TCF Scam Calls/SMS Description List to include the latest known scams. Any Code Signatory or Third Party can propose an update to the list by emailing info@tcf.org.nz.

17.4 When reviewing the TCF Scam Calls/SMS Description List the TCF should consider international information and best practice.

E Code Compliance

18 TCF Code Compliance Framework Obligations

18.1 The TCF, through its Code Compliance Framework (CCF) has the overall responsibility of ensuring that Code Signatories abide by the obligations set out in this Code.

18.2 The TCF CCF applies to the ongoing monitoring and compliance of this Code. By becoming a Code Signatory, Parties agree to comply with and are bound by the terms of the CCF and obligations set out in this Code.

18.3 The CCF's Complaints management procedures will apply to any allegations of a breach of this Code.

18.4 Self-certification Monitoring and Reporting Requirements

18.4.1 By signing up to this Code, Code Signatories agree to abide by the terms of the CCF and will cooperate in a full and frank manner with the Compliance Officer at all times, participate in good faith in any investigations they may be involved in and adhere to any sanctions levied against them under the CCF in relation to this Code.

18.4.2 In accordance with the CCF, Code Signatories must file initial and annual self-

certification forms with the Compliance Officer to demonstrate their initial and ongoing compliance with this Code.

18.4.3 It is the responsibility of the Parties to this Code to be fully conversant with the latest version of this Code, and to ensure that they are compliant at all times.

18.4.4 Each Code Signatory must keep information they deem necessary to show their compliance with this Code, should it be required.

18.5 Compliance Issue Management

18.5.1 The TCF CCF Section I sets out the process for dealing with notice of potential breach by a Code Signatory, investigation, sanctions and appeals process.

18.5.2 Parties who may provide notice of a potential breach of the Code to the TCF Code Compliance Officer is set out in s.I cl.28 of the CCF, including TDR who through their Complaints process may notify the Compliance Officer of a potential Code breach by a Code Signatory.

18.6 Telecommunications Act 2001

18.6.1 For the avoidance of doubt, the procedures set out in the CCF are additional to, and not exclusive of, any other rights a Party may have under the Telecommunications Act 2001, at law or in equity and nothing in the CCF will prevent any Party from exercising its rights to raise a dispute directly to the Commerce Commission in accordance with Part 4A of the Telecommunications Act 2001.

19 Expiry, Revocation and Amendment of the Code

19.1 The expiry, revocation or amendment of this Code will be in accordance with the New Zealand Telecommunications Forum's Operating Procedures Manual 'The Handbook', and TCF Member may put a Project Proposal to the Forum Board (at any time) for the amendment or revocation of the Code.

19.2 The Code will be reviewed every two years as required under the TCF CCF.

20 Code Signatory Self Certification Requirements

As part of the self-certification requirements of the CCF and this Code, parties must certify that they comply with the following Clauses of the Code:

All Code Signatories

a) Clause 9.2 Retail Service Providers will provide education information to Customers on their website warning Customers about scams and advising Customers where they can find additional information and how to report Scam Calling.
b) Clause 10.4 Network Operators will advise the TCF of contact details for Scam Calls and/or Scam SMS notifications.

Code Signatories using the TCF Scam Calls Notification Distribution List

a) Clause 11.1 Network Operators will only send a Scam Call Advisory Notice where they reasonably suspect the calls to be Scam Calls.
b) Clause 11.11 Network Operators will only send a Verified Scam Call Notice where there is enough evidence to confirm that the calls are highly likely to be Scam Calls.
c) Clause 11.14 Edge Networks will block calls on receipt of a Verified Scam Call Notice as soon as possible, and use reasonable efforts to block within two hours.
d) Clause 11.18 Network Operators will only send a Legitimate Call Notice if they can show that the traffic is legitimate.

Code Signatories using the TCF Scam SMS Notification Distribution List

a) Clause 13.5 Upstream Senders who receive a Verified Scam SMS Notice and take blocking action

must notify the affected Network Operator(s) by replying to the Notice to the Scam SMS Notification Distribution list.

b) Clause 13.6 Upstream Senders must send a Legitimate SMS Notice if they receive a Verified Scam SMS Notice for an individual SMS that they believe is legitimate.
c) Clause 14.1 Code Signatories will only send a Verified SMS Notice where they reasonably suspect the SMS to be Scam SMS.
d) Clause 14.3 Originating A2P SMS Partners will block the sender of the traffic on receipt of a Verified Scam SMS Notice as soon as possible and use reasonable efforts to block within two hours.
e) Clause 14.4 Network Operators will block the sender of the traffic on receipt of a Verified Scam SMS Notice, if they have the technical capability.
f) Clause 14.5 Network Operators who receive a Verified Scam SMS Notice and take blocking action must inform the affected A2P SMS Partners by replying to the Notice to the Scam SMS Notification Distribution list.
g) Clause 14.6 A2P SMS Partners will immediately block the traffic and send a Verified Scam SMS Notice when they confirm suspicious activity to be phishing or Scam SMS.
h) Clause 14.9 Originating A2P SMS Partners must send a Legitimate SMS Notice if they receive a Verified Scam SMS Notice for traffic that they believe is legitimate.

F Schedule 1: Suggested Call Blocking Methods, Response and Cause Codes

Several methods exist for blocking calling traffic once it has been deemed undesirable. This section discusses some methods available to carriers for blocking traffic in the context of the TCF Scam Prevention Code. It is intended as a guide for carriers, rather than being prescriptive, as capabilities and interoperability issues need to be taken into consideration. It does not cover details of the exact methods to implement traffic blocking.

Identifying which traffic to block

A crucial step is identifying which traffic is to be blocked, as the intent of traffic blocking is to stop malicious traffic without affecting normal service.

There are several pieces of metadata relating to any given call attempt which can be used to identify the traffic to be blocked or allowed. Below is a suggested list including scenarios where this might be useful, along with potential sources for the data.

Description	Scenario	SIP data source	SS7/ISDN data source
Calling Number (May be an individual DN, prefix or range)	Prevent Scam Calls which originate from specific calling number(s) or range(s)	From Header P-Asserted-ID Header RPID Header Diversion Header	Calling DN
Called Number (May be an individual DN, prefix or range)	Preventing callbacks or calls towards a known scam number or high-risk prefix	To Header Request-URI Header	Called DN
Source Trunk or Carrier	Traffic originating from specific carrier(s)	Source IP Address	Physical carrier

Blocking Traffic

Once a call has been identified for blocking using the available criteria there are several options available. Four suggested methods are discussed in the table below.

Action	Benefit / Cost
Reject call immediately with an appropriate response code	Simplest to implement Minimises Network impact
Play a message to the caller and disconnect the call with an appropriate response code	Requires media resource to play message Network impact is more than rejecting the call
Funnel the call to a "honey trap" to absorb the malicious party's resources	Requires media or human resource Increased Network impact
Divert the call to a known party to allow positive identification of the nature of the call	Useful for determining nature of calls

When rejecting a call, the aim is to prevent retry of the call via a second carrier or another available trunk. This may require some testing and/or discussion with upstream carriers to ensure their configuration specifies the expected behaviour. Suggested response codes / cause codes are provided below.

SIP Response [1]		Q.931 Cause [3][4]		Benefits / Risks
Code	**Text**	**Code**	**Description**	
607 [2]	Unwanted	-	N/A	Recommended by RFC 8197 [2] for unwanted traffic Relatively recent RFC, may not be well supported by all carriers or equipment
403	Forbidden	21	Call Rejected	Should work as intended in most scenarios May trigger overflow to alternate trunks or carriers
603	Decline	-	N/A	Alternative to above
404	Not Found	1	Unallocated or unassigned Number	Not technically correct however may prevent overflow May be more difficult to detect blocking by calling party as it appears as invalid number dialled
-	-	47	Resource unavailable, unspecified	May also be suitable for SS7/ISDN interconnects

Un-Blocking Traffic

Un-Blocking Traffic consists of removing the block and allowing the traffic to be treated normally again.

Audit Log

It is recommended that a log is kept of details used to perform blocking or un-blocking, at minimum the date and time the block was implemented, which user performed the blocking or un-blocking, and a brief description field.

This audit log is a useful tool if blocks are queried in the future.

Allowlisting traffic

When suspicious traffic is identified as being legitimate, you may wish to Allowlist the traffic.

Allowlisting is a way of notifying members that a particular number should not be blocked, preventing accidental blocking of legitimate traffic in these cases.

The Allowlist should contain details of the numbers to be Allowlisted, the date and time they were Allowlisted, which user updated the Allowlist, and a description field.

This Allowlist could prevent the accidental blocking of numbers, if it were integrated into the system which maintains the Blocking data.

References:

[1] RFC 3261 SIP: Session Initiation Protocol, section 21
[2] RFC 8197 A SIP Response Code for Unwanted Calls
[3] ITU-T Q.931, Appendix I; Definition of causes values
[4] ITU-T Q.850, Section 2.2.7; Cause definitions