New Zealand Telecommunications Forum

Code for Scam Calling Prevention

("Scam Calling Prevention Code")

Code Status:	Final (version 4)
Code Classification:	Voluntary Code
Date:	17 October 2019
Review Status:	Original version endorsed June 2018, V3 endorsed October 2019.

Introductory Statement

The New Zealand Telecommunications Forum Incorporated *Code for Scam Calling Prevention ("Scam Calling Prevention Code")* is a code for network operators to identify, verify and take action on scam calls to landlines and mobile phones.

Background

New Zealand, like many other countries, is targeted by off-shore based phone 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, and transfer it to the scammer's bank account.

Whilst an informally agreed process exists between Network Operators to identify and block international scammer activity, the industry would like to formalise this agreement and work more proactively and collaboratively (within industry and with relevant external bodies) to address the problem.

Anticipated benefits for Consumers

- Reduction in the number of scam calls received by customers and the harm that can result from these.

Anticipated benefits for Industry

- A consistent approach to identifying, verifying and blocking scam calls.
- Reduction in the number of instances of scam calls received by Network Operators.
- Minimised impact on legitimate traffic.

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 Calling Prevention Code ("Code") consists of:

a) **This Code** that sets out the scope, principles and requirements; and
b) The supporting **Scam Calls Description list** – a separate document for code signatories that will be updated as new scam call types are identified to support signatories 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.

TABLE OF CONTENTS

A Defined Terms

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 operator's switch to stop a call from progressing with the intended consequence of failing the call. Blocking may be performed on specific numbers or routes.
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 Calling Prevention Code
Code Signatory(s)	refers to a Network Operator that has signed up to this Code
Commencement Date	is the date set out in clause 12.1
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.
Edge Network	means the closest Network Operator(s) in New Zealand to the source. Typically, these will be Network Operators with international connectivity or domestic Network Operators where the scam originates within New Zealand.
Local Fibre Company	has the meaning set out in section 156AB of the Telecommunications Act 2001.
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 but excludes Local Fibre Companies
Person	means a legal person and includes a company and any other legal entity.
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 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 Calls Description List	means the list of scam calls agreed by the TCF which defines the characteristics of phone scams and the evidential standard required to identify them. The List of Scam Calls will be regularly updated on the TCF website as new scams are discovered.
TCF	means the New Zealand Telecommunications Forum Incorporated

Telecommunication(s) Service	means any good, service, equipment and/or facility that enables or facilitates Telecommunication.
Un-Blocking Traffic	means removing any Blocking Traffic restrictions applied.

B Introduction

1 Background

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

1.2 Some Network Operators in New Zealand have invested in a Scam Call prevention system to identify Scam Calls and/or have the capability to Block Traffic.

1.3 Network Operators block Scam Calls on their Networks for a variety of reasons including:

a) to protect Customers, or

b) to protect their Networks.

1.4 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 that traffic being carried by another Network Operator.

1.5 Network Operators Blocking Traffic will deter the incentives for scam calls in New Zealand and internationally.

2 Purpose

2.1 The purpose of this Code is to reduce the volume of Call Scams by stopping them as close as possible to their source.

2.2 It will establish coordinated sharing of Scam Call information between Networks in New Zealand and internationally to enable quicker responses and discourage scam calls.

2.3 It will minimise the impact of inbound and outbound Scam Calls on individual end users to reduce the risk of harm by making the public more aware of Scam Calls though the Scam Call Description List.

2.4 The Code will set out how Retail Service Providers and Network Operators will identify and communicate scam calling between each other so they can act to ultimately stop the calls.

2.5 The Code will help educate customers so they can identify and respond appropriately to Call Scams and provide a framework for the industry to identify new Scam Calls for inclusion on the Scam Calls Description List.

2.6 It also provides a means for industry to share information with key stakeholders, including law enforcement agencies, on Scam Calls for the purpose only of blocking or preventing Scam Calls.

3 Objectives

3.1 The objectives of this Code are to:

3.1.1 Minimise the impact of Scam Calls on individual end users to reduce the risk of harm.

3.1.2 Facilitate the timely sharing between Operators of agreed Scam Call information on the Scam Calling List.

3.1.3 Facilitate blocking of Scam Calls between Network Operators within New Zealand and internationally.

3.1.4 Specify a common process framework that Network Operators will use to share information on Scam Calling while complying with privacy legislation and Code confidentiality obligations.

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

3.1.6 To minimise the impact on legitimate traffic, including users whose numbers have been spoofed.

4 Scope

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

4.2 This Code also covers the sharing of Scam Call information for the purposes of investigating and blocking Scam Calls and/or the reporting of trends in scam calling for consumer education purposes, subject to compliance with section 6.4.

4.3 Un-blocking what were thought to be Scam Calls is an important part of the Customer experience enabling a Network Operator to ensure legitimate traffic resumes.

5 Exclusions from scope

5.1 This Code does not apply to:

5.1.1 Non-scam calls such as legitimate outbound sales calls or 2-factor authentication calls.

5.1.2 Malicious or nuisance calls that do not meet the definition of a Scam Call.

5.1.3 The blocking of email, online messaging or text messaging.

5.1.4 Revenue share fraud which is covered by TCF's International Revenue Share Fraud Guidelines.

5.1.5 Inter-Network Operator Fraud.

5.1.6 Local Fibre Companies and other providers of infrastructure that can be used to support telephony services but which are not best placed to Block Traffic or detect Scam Calls, except that any such organisations may be authorised as third parties in accordance with section 10.

6 Principles

6.1 This Code will facilitate ongoing coordinated sharing of Scam Call information between New Zealand Network Operators and will be used to facilitate any new Network Operator into the sharing arrangement.

6.2 Traffic Blocking and Unblocking Traffic will only occur in accordance with the agreed process set out in this Code.

6.3 Network Operators must not Block Traffic or Unblock Traffic in order to gain any commercial advantage or inflict any damage on any other Network Operator. Blocking Traffic or Unblocking Traffic cannot be used to withhold service or resolve commercial disputes (including bad debt scenarios).

6.4 In exercising their functions under this Code, Network Operators, Retail Service Providers and

third parties sending Third Party Notices must:

6.4.1 comply with all relevant privacy legislation; and

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

7 Retail Service Providers

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

7.2 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.

8 Implementation

8.1 Network Operators are responsible for how they detect Scams Calls on their own Network.

8.2 Network Operators who are the Edge Network are responsible for how they Block Traffic on their Network, but must do so in a way which minimises the impact on legitimate traffic.

8.3 Network Operators must keep track of Customer reports of Scam Calls.

8.4 Network Operators and Retail Service Providers will advise the TCF of their generic Scam Calls Notifications email address to be added to the TCF Scam Calls Notifications Distribution List used to notify each other of potential and actual Scam Calls.

9 Managing the Scam Calls

Sending a Scam Call Advisory Notice

9.1 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.

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

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

9.2.2 The characteristics of the scam.

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

9.2.4 Identify the upstream providers.

9.2.5 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.

9.3 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

9.4 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.

9.5 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.

9.6 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 providers to reach the Edge Network who is best placed to take action.

9.7 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 Calls Advisory Notice relates to a real Scam Call then they must send out a Verified Scam Call Notice to the Scam Calls Notification List as per Section 9.9.

9.8 Advisory Notices do not need to be acknowledged by recipients.

Sending a Verified Scam Call Notice

9.9 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.

9.10 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.

9.11 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.

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

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

9.12.2 The characteristics of the scam

9.12.3 Network traffic information

9.12.4 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.

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

9.12.6 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

9.13 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.

9.14 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 within two hours.

9.15 The Edge Network should notify their upstream provider, if relevant, that the Scam Calls have been blocked under this TCF Code.

9.16 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:

9.16.1 Date and time that blocking was actioned; and

9.16.2 Any other supporting/relevant notes.

9.16.3 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.

9.17 Calls should remain blocked for four (4) weeks after the Verified Scam Call Notice has been received. After this time the calls can be unblocked if the scam calls have stopped.

Legitimate Call Notice

9.18 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 List.

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

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

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

9.19.3 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.

9.20 If a Network Operator receives a Legitimate Call Notice and has Blocked Traffic they should Unblock Traffic.

Third Party Notice

9.21 A third party may be authorised to send Third Party Notices to Code Signatories in accordance with section 10.

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

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

9.22.2 The characteristics of the scam

9.22.3 Network traffic information

9.22.4 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.

9.22.5 The organisation names of any Retail Service Provider(s) and/or Network Operator(s) involved in the investigation.

9.22.6 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.

9.22.7 Contact information of the Third Party sending the notice.

10 Third Party Engagement

10.1 The TCF may permit third parties (e.g. government agencies, online safety organisations) to receive Verified Scam Call 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.

10.2 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.

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

10.4 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.

10.5 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.

10.6 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.

C Scam Calls Description

11 Scam Calls Description List

11.1 The evidential standard for scams is defined in the TCF Scam Calls Description List.

11.2 The TCF Scam Calls Description List will include:

11.2.1 The description of the scam and its key characteristics

11.2.2 The evidential standard for identifying the scam including e.g. flow rates.

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

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

D Code Compliance & Administration

12 Commencement and Compliance

12.1 This Code shall come into force once endorsed by the TCF Board.

12.2 The TCF Code Compliance Framework (CCF) applies to the ongoing monitoring and compliance of this Code. By becoming a Code Signatory, Code Signatories agree to comply with and are bound by the terms of the CCF in relation to the performance of their obligations under this Code.

12.3 For the purposes of the self-certification requirements under the CCF, the key metrics of this Code that Code Signatories are required to self-certify they comply with are set out in Schedule 1.

12.4 Parties that sign up to this Code after it comes into force will have one (1) month from the date of signing to make any necessary changes to comply with the requirements of the Code.

12.5 The CCF's complaints management procedures will apply to any allegations of a breach of this Code, made by one Code Signatory about another to the Compliance Officer. 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.

12.6 In the event of any inconsistency between this Code, any relevant legislation, and any relevant requirements, this inconsistency will be resolved in the following (descending) order of precedence:

12.6.1 Any legislation, and

12.6.2 This Code.

12.7 This Code contains the minimum requirements regarding the blocking of Scam Calls between Network Operators. Network Operators may agree to adhere to a higher standard as part of any bilateral agreement reached between themselves from time to time.

13 Revocation and Amendment of the Code

13.1 In accordance with the TCF's Operating Procedures Manual, any TCF member may put a project proposal to the TCF Board (at any time) for the amendment or revocation of this Code. If you wish to propose changes to this Code, please contact info@tcf.org.nz

13.2 The TCF will undertake a review of this Code one (1) year from the Commencement Date in order to assess the extent to which it is achieving its aims and objectives and any other relevant matter pertinent to the operation of this Code. Following this review, the TCF may undertake amendments to this Code as required, in accordance with the procedures set out in the TCF Rules and Handbook.

14 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:

1 Clause 6.3 Network Operators and Retail Service Providers shall not block or request to block calls in order to gain any commercial advantage or inflict any damage.
2 Clause 7.2 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
3 Clause 8.4 Network Operators will advise the TCF of contact details for scam calls notifications.
4 Clause 9.1 Network Operators will only send a Scam Call Advisory Notice where they have that they reasonable suspect to be Scam Calls.
5 Clause 9.11 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.
6 Clause 9.14 Edge will block calls on receipt of a Verified Scam Call Notice within two hours.
7 Clause 9.18 Network Operators will only send a Legitimate Call Notice if they can show that the traffic is legitimate.

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

E 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 Call 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

Unblocking traffic

Unblocking 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 unblocking, at minimum the date and time the block was implemented, which user performed the blocking or unblocking, and a brief description field.

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

Whitelisting traffic

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

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

The Whitelist should contain details of the calls to be whitelisted, the date and time they were whitelisted, which user updated the whitelist, and a description field.

This Whitelist 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