
**New Zealand Telecommunications Forum Inc**

# Telecommunications International Revenue Share Fraud Prevention Guidelines ("IRSF Prevention Guidelines")

| **DOCUMENT VERSION:** | |
|---|---|
| Number and Status: | **Endorsed** |
| Date: | 28 April 2016 |
| Code Classification: | TCF Guideline |
| Prepared by: | IRSF Working Party |

## INTRODUCTORY STATEMENT

This is the first version of the *Telecommunications International Revenue Share Fraud Prevention Guidelines ('Guidelines)*.

The Guidelines set out a best practice approach framework for the mitigation of international revenue share fraud (IRSF) by New Zealand telecommunications service providers.

For the purposes of these Guidelines, '*revenue share fraud*' describes any type of fraudulent offending that involves the generation of telecommunications with intent to dishonestly benefit from interconnect charges. It therefore includes such crimes as PABX hacking, IRSF, Wangiri fraud, VoIP hacking and voicemail hacking.

The Guidelines are designed to assist the coordination of efforts by network operators, service providers, carriers and other stakeholders to combat the fraud by establishing a best practice framework for these groups to refer to when taking steps to combat IRSF

The single most effective way to reduce the likelihood of being a victim of fraud is for a Customer to ensure their equipment is appropriately configured and protected. As a result these Guidelines suggest that the industry provides up-to-date guidance on the steps Customers can take to protect themselves from fraud.

This combined approach seeks to reduce the opportunities and benefits of fraud and it is the industry's hope that it can effectively eliminate these types of fraud from the New Zealand telecommunications sector.

**Background**
The global cost of international revenue share fraud to the telecommunications industry has been reported by the Communications Fraud Control Association (CFCA) as US$10.8 billion in 2015[1].

The issue of IRSF and PABX hacking remains a concern for telecommunications providers and for their Customers who can both face considerable financial loss and business disruption.

**Anticipated benefits for Customers**
- Reduction in financial loss and business disruption from IRSF by:
  - Informed Customers taking appropriate steps to protect themselves.
  - Industry working together to identify and address instances of IRSF.

**Anticipated benefits for Industry**
- Better informed Customers taking steps to protect themselves from IRSF.
- Closer industry collaboration and cooperation to reduce revenue loss and business disruption through IRSF.

**Guideline Revision**
This is the first iteration of the Guidelines.

[1] http://cfca.org/fraudlosssurvey/2015.pdf

# CONTENTS

## A. ACRONYMS AND DEFINITIONS

The following acronyms and definitions apply to these Guidelines.

| | |
|---|---|
| **Billing Relationship** | means a relationship where the Service Provider has a bona fide right to charge the Customer for any chargeable activity relating to the provision of Telecommunications Services. |
| **Business Day** | means a day on which registered New Zealand banks are open for normal banking business, excluding Saturdays, Sundays and nation-wide New Zealand public holidays. Regional public holidays are considered to be Business Days. |
| **Guidelines** | means these Guidelines. |
| **Customer** | means a party who has a bona fide Billing Relationship with a Service Provider in respect of a Telecommunications Service. |
| **Fraudulent Communication(s)** | means any electronic communication that originates from, is carried across, or terminates on any telecommunications network or systems, and which has been generated for the purpose of obtaining revenue by deception, trick or other dishonest stratagem. It includes activities such as PABX hacking, IRSF, Wangiri fraud, VoIP hacking and voicemail hacking. |
| **GSMA** | means GSM Association. |
| **GSM** | means Global System for Mobile Communications. |
| **International Revenue Share Fraud** | means the artificial inflation of traffic to certain international number ranges with no intention to pay for the calls (or paying where there exists some form of arbitrage opportunity), or by stimulating calls by others to the number ranges. The fraudster receives a share of the revenue from termination charges obtained by the number range holder for inbound traffic to the number ranges. |
| **IRSF** | means International Revenue Share Fraud. |
| **PABX** | means Private Automatic Branch Exchange. |
| **Service Provider** | means any party providing a Telecommunication Service to a Customer and who has the Billing Relationship with the Customer for that service. |
| **TCF** | means the New Zealand Telecommunications Forum Incorporated. |
| **Telecommunication(s) Service** | means any good, service, equipment and/or facility that enables or facilitates telecommunication. |
| **VoIP** | means Voice over Internet Protocol. |
| **Wangiri Fraud** | means a type of telecommunications fraud where an automated system dials a large number of phone numbers, usually mobiles and hangs up before the recipient can answer. The number appears as a missed call on the recipient's phones. If a recipient calls the missed number back, they are either charged a premium rate or hear an advertising message. |

## B. PURPOSE

1. The purpose of these Guidelines is to reduce or eliminate the incidence and effects of IRSF on New Zealand Telecommunications Service Providers and their Customers by providing a best practice framework for Service Providers to use when seeking to mitigate telecommunications revenue share fraud.

## C. OBJECTIVES

2. The objective of the Guidelines is to set out the minimum standards for:

   2.1. Educating Customers about IRSF.

   2.2. Sharing information between Telecommunications Service Providers that may assist them to identify, avoid, or mitigate the effects of IRSF.

   2.3. Detection and mitigation capability that Telecommunication Service Providers should have in place to support the purpose of these Guidelines.

## D. SCOPE

3. These Guidelines provide a framework for New Zealand Telecommunication Service Providers who are committed to addressing the issue of International Revenue Share Fraud.

## E. PRINCIPLES

4. The following principles should be applied by Service Providers when interpreting these Guidelines. Service providers should:

   4.1. act in good faith at all times;

   4.2. at all times seek to protect the welfare of their Customers, including through the provision of information and educational material about the risks of IRSF;

   4.3. act within applicable laws;

   4.4. alert the TCF when a significant increase in fraudulent communications becomes evident;

   4.5. cooperate with other Service Providers in the prevention, investigation and mitigation of IRSF or other communications fraud; and,

   4.6. cooperate with law enforcement agencies in the investigation and prosecution of IRSF and other communications fraud.

## F. EDUCATING CUSTOMERS TO PREVENT FRAUDULENT COMMUNICATIONS

5. To educate Customers about how they can prevent Fraudulent Communications, Service Providers should provide up-to-date information for Customers on their public websites detailing:

   5.1. The types of communication fraud risks Customers may be exposed to;

   5.2. The steps Customers can take to mitigate those risks, such as:

      (i) Changing default PINs and passwords on newly acquired equipment

      (ii) Selecting strong PINS and passwords (e.g. Not “1234” or “0000” or “password” etc.)

      (iii) Locking mobile handsets and SIM cards with secure PINs

      (iv) Ensuring that voicemail PINs are secure;

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

(vi) Changing PINs and passwords regularly;

(vii) Not responding to missed calls from international or unknown local numbers; and,

(viii) Not responding by landline or mobile phone to SMSs they receive from unknown mobile numbers.

5.3. The actions that Customers should take if they find that they have fallen victim to such offending.

## G. IDENTIFICATION AND MITIGATION OF FRAUDULENT COMMUNICATIONS

6. Service Providers should have in place detection systems that will monitor and identify anomalous communication patterns that exhibit characteristics of Fraudulent Communications.

7. Service Providers should, as soon as reasonably practicable, attempt to identify whether or not any such anomalous communication patterns detected were fraudulent.

8. Service Providers who detect and confirm Fraudulent Communications originating from, passing across, or terminating on their systems, should use reasonable endeavours to immediately block any further such traffic originating from and/or destined to the same parties.

## H. SHARING INFORMATION ABOUT FRAUDULENT COMMUNICATIONS

9. Service Providers should share up-to-date details of their Fraud Teams with each other to facilitate information sharing about Fraudulent Communications.

10. The TCF will maintain an opt-in contact list and email distribution list for the purpose of sharing the information outlined in clause 9 between participating Service Providers.

11. A list of participating Service Providers will be made available on a password protected page on the TCF website: www.tcf.org.nz.

12. Following the successful blocking of Fraudulent Communications, Service Providers should, within two Business Days of identifying the fraudulent activity, share with other Service Providers details relating to the incident. The type of information that should typically be shared includes:

12.1. the name of the network the Fraudulent Communications occurred on;

12.2. the date and time of occurrence;

12.3. the type of fraud detected;

12.4. the individual overseas numbers the Fraudulent Communications were made to or originated from;

12.5. if identified, the overseas numbers making the hacking calls into the Customer's PABX if applicable;

12.6. the action taken by the Service Provider;

12.7. the contact details for the person to contact with any queries; and,

12.8. any other relevant information available.

13. A sample email template setting out the information in clause 9 has been provided for Service Providers use in Appendix 1.

## 14. Expiry, Revocation and Amendment of the Guidelines

14.1. For the avoidance of doubt, and in accordance with the New Zealand Telecommunications Forum Operating Procedures Manual, any TCF Member may put a Project Proposal to the TCF Board at any time for the amendment or revocation of these Guidelines.

14.2. Any enquiries or advice in relation to these Guidelines can be made at www.tcf.org.nz/contact.

# I. APPENDIX 1

## Sample Email Template for Sharing Information about Fraudulent Communications between Service Providers

Subject: TCF IRSF > [Company Name] > IRSF Notification

Email Body:

In accordance with section H of the TCF IRSF Prevention Guidelines, below is information about an IRSF related incident that occurred on our network.

Date and time of occurrence:
**[DD MONTH YYYY HH:MM]**

Fraud type detected:
**[Insert fraud type here]**

Overseas Numbers the fraudulent communications were made to:
**[List numbers/number block here]**

The overseas numbers making the hacking calls into the Customer's PABX if applicable
**[Details here or state Not Applicable or Unknown]**

Action taken
**[Detail the action you have taken here]**

Other Details
**[Any other relevant information available]**

For more information please contact:
**[Contact details for the person to contact with any queries]**