Intercarrier Process in relation to Internet Dumping

1. Purpose

The purpose of this Intercarrier Process document ('the Process") relates to the sharing of destination information as between suppliers where there is a reasonable belief that there is traffic that is of a suspicious nature. At the end of this document is an Attachment which sets out the suggested text to be included in any email 'alert' sent between suppliers.

2. Introduction

What is Internet dumping?

Internet dumping is where an internet user is disconnected from their local call modem connection to an ISP and, by means of an automatic dialler, reconnected to a website which, in most cases, terminates on an international mobile or international fixed line number. In the past, the call was often connected to 1900 numbers, but in recent times, driven by some carriers' removal of access to 1900 services, these calls have been connected to international numbers either directly, using the 0011 prefix, or via other carriers using the applicable override code.

This is typically traffic generated by automatic diallers associated with Internet dumping, but could also be of other nature.

One of the issues that suppliers have become aware of is that we have anecdotal evidence of, in some instances, the PC speaker being muted as part of the dumping programme's characteristics. This also prevents the computer user hearing any call progress tones (dial tone, supervision tones, supervisory tones, international call connect tone sequence) that indicate that they are placing an unintended long distance / international call.

As a result of industry concern, this Process is designed to document the protocol for the handling of information between suppliers.

3. Sourcing of information

Typically, information leading to number ranges associated with this type of practice could come from one of the following areas:

- Customer: upon the receipt of a bill that contains calls not recognised by the customer or the bill amount is significantly higher than expected, customers will contact their respective supplier's Front of House ('FOH') /Customer Service to investigate the cause;

- Supplier Billing: Significant changes in the amount of one bill compared to another detected by the Supplier. The customer may/may not be proactively informed via a courtesy call;

- Supplier technical: Changes in traffic patterns to international destinations, detected automatically or manually by the Supplier. Where the destination is a known target, or the usual traffic pattern is generally of a low volume, detection is relatively easy to see. Where there is traditionally a large amount of traffic, the change due to dumping is less likely to be seen and thus is likely to remain undetected for longer (if it is detected at all);

- Supplier Fraud unit detection – who have their own detection tools;

- TIO advice where the customer approaches them directly; and

- Other supplier – where one of the sources above results in notice to the supplier of potential Internet Dumping activities.

4. Number range blocking

Each supplier should carefully consider the commercial and customer consequences of blocking and the potential loss of revenue.

Consequences of blocking number ranges for carriers:

- **Technical**

Occupation of space in number range blocking facilities – there is finite amount of space in the equipment for blocking instructions and thus the decision to block and the size of the number ranges to be blocked should be carefully considered. The equipment has a limited capacity for blocking instructions.

- **Commercial: Unintended and don't pay**

The bill payer/internet user did not intend to make the calls and are genuinely surprised when the calls appear on the bill.

They contact FOH/Customer Service and challenge the charge and generally have the call charge waived. This presents a commercial risk to the supplier as the international minutes need to be paid for and the relevant carrier will have no revenue associated with them. If a rebate is not granted to the customer, these calls present a public relations risk to the supplier as these customers may take the issue to the media. In general, most suppliers' FOH staff have limited access to rebate amounts.

- **Commercial: Unintended and pay**

Some customers, especially where the bill is not large or there are a large number of similar calls, may not notice the unintended calls and simply pay for the calls.

- **Intended and challenge**

A percentage of calls will be challenged despite the caller's intentional calling and where the customer tries to obtain the calls for free.

- **Intended and pay**

If blocking is invoked, these lost calling opportunities represent a commercial risk to the supplier, as the supplier loses the opportunity to make revenue from genuine callers to the blocked number ranges.

Customer consequences:

The customer attempts to dial blocked numbers will fail in the network (a voice caller would hear either Number Unobtainable tone or a recorded message) but there is the possibility of blocking legitimate numbers. Each supplier should develop its own internal protocol to manage all complaints and issues that arise if legitimate numbers are blocked.

The host of the destination websites:

The hosts of the destination websites may suffer a loss of revenue if a supplier decides to block access to their terminating numbers. It is likely that they may complain to the relevant supplier or a regulator such as the ACA or the ACCC about their lack of access their services.

5. Investigation

Each supplier should consider what he or she wishes to do with number range information that they have not detected and have received from another supplier. This information should be investigated thoroughly by the supplier if they are considering acting on that information. They should use all resources that they see fit to confirm the information and they should act based upon their investigations.

The Process could include the following:

- monitoring the traffic pattern to the destination using historic data;
- a judgement on whether the traffic is legitimate and if not, whether it warrants blocking;
- if the decision to block is made, how many numbers to block & for how long.

6. Call dumping Patterns

Dumped calls have been identified as having one or more of the following characteristics (*Note: there may be other characteristics of dumping that that have not been observed, so this list should not be considered exhaustive)*:

- A large change in calling patterns to a destination very quickly. In some cases, a 5 fold increase in the minutes of use to a destination in a matter of days has been observed;

- High call completion rates. The providers of these services want all calls answered thus overprovision the services leading to above-average call completion rates;

- Some destinations are recognised as typical dumping destinations. Known reasons range from receptive destination telcos to high call termination charges and superfluous vacant number ranges. Supplier experience suggests a recent trend in dumped traffic going to non-traditional destinations, despite the less lucrative nature of such traffic. In the past, it has been difficult to detect this type of traffic;

- Specific calling patterns. If it observed that a call to an ISP is cut off, and then a call to an international number follows almost immediately (i.e. within ~10 seconds) a dumping event is likely to be the cause; and

- Calls of a specific duration. Calls that are disconnected within a few seconds of 30 minutes (or multiples thereof) have been observed and identified as dumped. It should be noted that some destination countries have call duration limits imposed to conserve their network resources and this indicator of potential dumping should be used with caution.

7. Actions

Suppliers should rely on their own resources to detect, investigate and act upon information received. Each supplier must consider the commercial and customer impacts of any proposed action. An action plan in the case of adverse public reaction should also be considered.

It is recommended that any blocking processes undertaken by a supplier should be reviewed on a regular basis.

8. Transfer of information

Alerts relating to number range information for *inter* supplier use, should use the agreed template (See Attachment 1).

Intra supplier information distribution is to be in accordance with that supplier's internal processes.

9. Disconnect/reconnect

The format and process for disconnect & reconnect of number ranges should be the same: the supplier should investigate and satisfy itself as to whether the number range should be re-enabled.

Disconnection or blocking of number ranges should be done based on the supplier's own investigations.

Once a suspect number is detected, the range of numbers to be blocked should be determined.

The size of the number range to be blocked should be considered based upon customer feedback and how widespread the detection of modem tones in a number range is.

10. Review

Records of blocked number ranges should be retained and the evidence of investigations should be retained to support customer/authority complaint instances.

11. Customer complaints

Complaints about billed calls as well as the inability to access blocked numbers should be dealt with based on the supplier's existing policies.

Attachment 1

Suggested text for inter-supplier email **alert** by authorised representative from each supplier:

[insert date]

Sir/Madam,

We have observed an unusual traffic pattern to the following number ranges(s):

Country Code:	(+) xx
Number range From:	xxx xxxx xxxx
Number range To:	xxx xxxx xxxx

This information is provided as advice only, you must carry out your own investigations to ascertain the nature of this traffic and the range of numbers affected. Please note that this traffic was observed recently but the pattern of usage may have changed since our traffic measurement.

All care has been taken in the observations above, and the compilation of this communication. Any action taken by [insert name of supplier] should be done in accordance with your own internal processes and policies and any decision to block number ranges shall be based on the results of your own investigations.