November 2005

ETNO Reflection Document on Best Common Practice for Numbering Misuse Protection

Executive Summary

The European Telecommunications Network Operators' Association [1] (ETNO) supports Study Group 2 chairman's proposal in developing guidelines for Member States and Sector Members to combat misuse (COM 2 – C 21 - Draft new annex for E.misuse). ETNO welcomes this opportunity to offer their views on numbering misuse and share experience of some of its members in taking preventive measures against certain types of numbering misuse. This contribution proposes text for inclusion in a possible annex to E.misuse. The document discusses the different dimensions that must be considered in tackling numbering misuse and elaborates on concrete measures that can be taken specifically against "rogue diallers". However, with regard to the section on refund policies, ETNO believes that this is a commercial issue between the consumer and the service provider, and should not be discussed in detail in the best practice Annex.

Proposed text for Annex on best common practice

1. Numbering misuse

1.1 Rationale

E.164 numbering misuse takes several forms and is detrimental to the industry in various respects. Unfortunately, there is no single measure to tackle this practice as a whole and all potential actions should be considered. The choice of measure or measures may also depend upon the national circumstances, the state of the network and the extent of the problem. In order of importance, the measures against numbering misuse should be to:

1. protect customers against frauds, applying measures from security warnings to deploying automatic dialup protection mechanisms.

[1] ETNO is the recognised voice of the European Telecommunications network operators with over a decade of experience in shaping EU telecoms policy. The association represents 41 companies from 34 European countries. They account for an aggregate turnover of more than 210 billion Euros within Europe and employ more than one million people. The association is widely recognised for its expertise on various topics including technical and regulatory matters, but also issues such as network naming and addressing, environmental protection, sustainability and network security.

2. protect service providers and operators against revenue frauds with measures such as:
    - Revenue protection procedures
    - Cooperation with transit and terminating network operators
    - Call barring whenever appropriate
    - Obligations for terminating service providers towards customers: clear price indication, agreement by customer to set up expensive calls, etc…
3. prevent future numbering misuses by controlling that E.164 CC assignee effectively uses the resources in a manner which is compliant with the purpose for which it was assigned. For this, the ITU has a prominent role to play to make sure that resources are used according to E.164 principles.

The responsibility of service providers is not addressed in this document.

1.2 National variations

Depending on the country, call termination obligations to national and/or foreign destinations (both geographic and non geographic) may exist. These should not be counterproductive when dealing with misuse, premium rate or revenue share number frauds. When abuse and frauds are detected, customer protection should take precedence over such call termination obligations. However, since national regulatory regimes sometimes differ, actions may also differ from country to country in this area.

National authorities should be encouraged to state their positions on "notoriously abused" destinations (eg ComReg policy[2] later withdrawn) and administrations should also be encouraged to assist in controlling misuse. For example, identifying and barring calls to destinations that have been recognised as being misused.

1.3 Refund policies

The area of Refund policies is one that is rightly addressed as part of the commercial relationship between Service Providers and customers, and as such has to take account of a wide range of issues. ETNO believes that this section has to take into account a number of factors to ensure that no one party profits from misuse, and parties involved recognise their individual responsibilities. These factors are often commercial and not technical.

1.4 Call barring

Selective call barring by a network operator may prove effective against numbering frauds, as the customers can not reach the service provider through the numbering resource / code assignee, or to protect operators' customers as soon as the abuse is detected.

From the technical point of view, it is important to note that limitations on call barring may exist in practice. Generally speaking, single numbering barring is hardly ever technically and economically feasible and as diallers normally use more than one number is not effective. Within some instances call barring to international blocks may prove to be the only possibility.

---

[2] See note http://www.comreg.ie/_fileupload/publications/ComReg0499.pdf. The document also offers a number of possible measures against number misuse.

Such an approach should be periodically reviewed to make sure the misuse is properly and proportionately addressed.

2 Preventing premium rate rogue dialler frauds

2.1 Definition

A program that makes it possible for a computer to set up a call on the PSTN is generally referred to as a *web dialler*. Some of these web diallers are used fraudulently to establish calls to high-termination fee numbers such as national, international or satellite destinations. This fraud is generally referred to as premium rate rogue dialler fraud. A rogue dialler is a piece of software, which is downloaded from the Internet and installed on a computer generally without the user's consent. The program changes the users' dial-up settings to an international number or a premium rate number.

Rogue diallers use an Internet Service Provider (ISP) Internet connection to install automatic diallers, which will then set up calls on a traditional Telephony Service Provider (TSP) service. The fact that the fraud involves two different kinds of players makes it sometimes difficult to deal with and calls for coordinated actions. The following elements propose preventive measures that can be applied by both ISPs and TSPs.

2.2 Preventive measures

2.2.1 Customer warnings

Operators and Internet Service providers should be encouraged to issue regular warnings and safety procedures to their customers. For all web diallers, technical preventive measures can be used by ISP customers such as:

- Install regular antivirus updates from your ISP or a source that can be considered as reliable
- Install stop-diallers freeware from your ISP or a source that can be considered as reliable
- Use firewall with the appropriate configuration
- Use automatic operating system updates and antivirus updates
- Advise customers not to systematically ignore security warnings

In addition, ISP customers using ISP dialup Internet connection numbers should be regularly advised to check that their dialup number has not been modified.

Broadband customers should disconnect dialup Internet connection. They should make sure that such connection is disabled if the computer modem supports dual-mode. Most customers may not be aware that web diallers cannot be used on broadband. Some customers still need the dial-up modem for fax communications.

2.2.2 Additional measures

The great majority of TSPs are victims of web dialler frauds and do not benefit from such abuse - TSPs have no information regarding the nature of the value-added services that are provided on such numbers.

They should also be free to apply call screening and international numbering block (i.e. CC for networks or geographic areas) or short code barring in

presence of elements indicating that fraudulent use is taking place (it is often proven more efficient to anticipate the fraud rather than reacting when the fraud is taking place). Most numbering abuse use portions of country codes. TSP can monitor suspected codes and bar incriminated destinations in a proportionate manner whenever appropriate (e.g. as soon as customers complaints are produced or worse, legal actions engaged).

Specific services can also be used to prevent web diallers such as:

- Selective call screening: most TSPs have service offering options that make it possible to restrict international destination calls. These services can be used to prevent unsolicited call setups to destinations such as satellite number or country codes notoriously used for web diallers.
- Where customers are offered calls, before setting up or accepting such calls, they should check the corresponding tariffs (customers can easily check the applicable tariffs on the operator website or a dedicated freephone service). It is therefore also important that the user is aware of the number that is being dialled and in particular, for international calls the suggested destination country code.
- Some TSPs provide services to monitor in real time calls and invoices to detect potential fraudulent behaviour.