International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

E.156

Supplement 1

(11/2007)

SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

International operation – Operation of international telephone services

---

Guidelines for ITU-T action on reported misuse of E.164 number resources

Supplement 1: Best practice guide on countering misuse of E.164 number resources

ITU-T Recommendation E.156 – Supplement 1

ITU-T

International Telecommunication Union

ITU-T E-SERIES RECOMMENDATIONS

OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS

INTERNATIONAL OPERATION	
Definitions	E.100–E.103
General provisions concerning Administrations	E.104–E.119
General provisions concerning users	E.120–E.139
Operation of international telephone services	**E.140–E.159**
Numbering plan of the international telephone service	E.160–E.169
International routing plan	E.170–E.179
Tones in national signalling systems	E.180–E.189
Numbering plan of the international telephone service	E.190–E.199
Maritime mobile service and public land mobile service	E.200–E.229
OPERATIONAL PROVISIONS RELATING TO CHARGING AND ACCOUNTING IN THE INTERNATIONAL TELEPHONE SERVICE	
Charging in the international telephone service	E.230–E.249
Measuring and recording call durations for accounting purposes	E.260–E.269
UTILIZATION OF THE INTERNATIONAL TELEPHONE NETWORK FOR NON-TELEPHONY APPLICATIONS	
General	E.300–E.319
Phototelegraphy	E.320–E.329
ISDN PROVISIONS CONCERNING USERS	E.330–E.349
INTERNATIONAL ROUTING PLAN	E.350–E.399
NETWORK MANAGEMENT	
International service statistics	E.400–E.404
International network management	E.405–E.419
Checking the quality of the international telephone service	E.420–E.489
TRAFFIC ENGINEERING	
Measurement and recording of traffic	E.490–E.505
Forecasting of traffic	E.506–E.509
Determination of the number of circuits in manual operation	E.510–E.519
Determination of the number of circuits in automatic and semi-automatic operation	E.520–E.539
Grade of service	E.540–E.599
Definitions	E.600–E.649
Traffic engineering for IP-networks	E.650–E.699
ISDN traffic engineering	E.700–E.749
Mobile network traffic engineering	E.750–E.799
QUALITY OF TELECOMMUNICATION SERVICES: CONCEPTS, MODELS, OBJECTIVES AND DEPENDABILITY PLANNING	
Terms and definitions related to the quality of telecommunication services	E.800–E.809
Models for telecommunication services	E.810–E.844
Objectives for quality of service and related concepts of telecommunication services	E.845–E.859
Use of quality of service objectives for planning of telecommunication networks	E.860–E.879
Field data collection and evaluation on the performance of equipment, networks and services	E.880–E.899
OTHER	E.900–E.999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation E.156

Guidelines for ITU-T action on reported misuse of E.164 number resources

Supplement 1

Best practice guide on countering misuse of E.164 number resources

Summary

This Best Practice Guide is intended as a complimentary volume to ITU-T Recommendation E.156 "Guidelines for ITU-T action on reported misuse of E.164 number resources" that specifies the measures that the ITU TSB will undertake with respect to reported alleged misuse of numbering resources over which it has some control.

This guide is intended to discuss what action other stakeholders may wish to take with regard to minimizing and managing the impact of misuse of numbering resources for their customers benefit.

Source

Supplement 1 to ITU-T Recommendation E.156 was agreed on 8 November 2007 by ITU-T Study Group 2 (2005-2008).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

CONTENTS

Introduction

This Best Practice Guide is intended as a complimentary volume to ITU-T Recommendation E.156 "Guidelines for ITU-T action on reported misuse of E.164 number resources" that specifies the measures that the ITU TSB will undertake with respect to reported alleged misuse of numbering resources over which it has some control.

This guide is intended to discuss what action other stakeholders may wish to take with regard to minimizing and managing the impact of misuse of numbering resources for their customers benefit. In order to identify what such best practice is, it will be useful to present some background on the issues associated with misuse.

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 majority of misuse of numbers is carried out independent of Internet diallers.

ITU-T Recommendation E.156

Guidelines for ITU-T action on reported misuse of E.164 number resources

Supplement 1

Best practice guide on countering misuse of E.164 number resources

1 Scope

This guide describes examples of misuse associated with E.164 numbering resources, together with descriptions of best practice to counter misuse. It was considered useful at the time it was written, and is intended to be used by Service providers and Regulators.

2 References

[ITU-T E.156] ITU-T Recommendation E.156 (2006), *Guidelines for ITU-T action on reported misuse of E.164 number resources*.

3 Acronyms

CRM Customer Relationship/Management

IDD International Direct Dial

IRSF International Revenue Share Forum

PRSP Premium Rate Service Provider

ROA Recognized Operating Agency

SIM Subscriber Identity Module

SMS Short Message Service

SP Service Provider(s)

TSP Telephony Service Provider

4 Distinguishing misuse and fraud

This clause distinguishes between misuse of numbering and fraud that were seen to exist at the time that the guide was written. It is recognized that it is not complete and that other activities will emerge that could be categorized as either misuse or fraud or both in the future. The information in this guide is sufficiently generic to be relevant.

It is not the purpose of this guide to describe in detail what is meant by fraud. Rather it is intended to show that the misuse of Numbers and numbering plans might form the basis by which a fraud is perpetrated but the misuse itself might not constitute actual fraud. For the purposes of this guide, misuse, associated with numbers, is defined as the use of numbers other than for what they are intended. Fraud, on the other hand, is use of numbers in the manner for which they were prescribed, but in a manner intended to generate revenue.

Table 1 – Relationship of number ranges and mechanisms to misuse and/or fraud

	Misuse: A Number or number range that is being used for a purpose other than for which it was allocated	**Misuse of a number in a fraudulent way**	**Fraud:** The use of a number in the manner for which it was allocated but for the purpose of generating cash at the expense of the customer and/or operators
Global numbering resources	Yes	Yes	Yes
International numbering resources	Yes • Example 1 Short stopping (to be defined) • Example 2 Mobile numbers could be misused as premium rate services on international level	Yes • Getting the consumer to instigate calls with short stopping	Yes • Example 1 Getting the consumer to instigate calls (to be defined)
National numbering resources	Yes Personal Numbers that have premium rate charges associated with them	Yes Instigating calls by the consumer to PNs that have premium rate charges associated with them	Yes • Example 1 Instigating calls to consumers to perceived expensive calls • Example 2 Calls to numbers incurring expensive call charges and exploiting settlement dates to receive payment from operators prior to the call origination costs being settled. (Note 1)
Local numbering resources	?	?	?
Advertisement	Yes	Yes	Yes
SMS	Yes	Yes	Yes
Rogue dialling (Note 2)	Yes	Yes	Yes

NOTE 1 – This example is included here to demonstrate that fraud can occur elsewhere in the end-to-end connectivity chain. Its inclusion here is for completeness, and whilst issues may appear to be similar to those of this guide, they are addressed elsewhere.

NOTE 2 – This table is intended to show that where fraud occurs, it should be dealt with as fraud, according to the laws that pertain. However, in some circumstances fraud occurs with numbering misuse, and other avenues are open to the operator/service provider in order to address the issue at hand by seeking to restrict the use of the number.

It is possible, for example, with a certain class of number (e.g., 882) to have an allocation that is being both misused, in that the original allocation did not necessarily allow for Internet access, for which the number is being used, and in association with an Internet or rogue dialler, the consumer has no control over the calls being made.

A further example of numbering misuse is where the numbers being used have a commercial surround, e.g., revenue sharing, and high termination rates, such that activities are used to stimulate calls to those numbers for the purpose of generating revenue. In this instance, the originator has decided to dial the digits, but it is based on fraudulent information.

It is probably much simpler to address 'misuse' than fraud because there are rules and procedures for the use of numbers and numbering plans. This implies that anything that does not comply with the rules and procedures is by definition 'misuse'. However, rules and procedures could be changed so that a use which was originally 'misuse' could subsequently be brought within the scope of new rules and procedures, and thus becomes another permitted 'use' of the numbers and numbering plan.

5 Issues

This clause details the issues that arise from specific instances of misuse that are known at the time of approval of the guide, and offers some guidance that can be taken by various stakeholders to resolve the issues.

The issues of misuse can emerge from:

a) premium rate services (see clause 5.1);

b) telephone number misuse (see clause 5.2);

c) mobile (see clause 5.3).

5.1 Premium rate services

Premium rate services are used with both normal calls and SMS messages, and can be accessed using national and international numbering resources.

Common applications for calls are:

- recorded information;
- live professional advice (e.g., legal advice, health advice);
- tele-voting;
- complaint lines[1] and customer service/advice lines (e.g., software support);
- games and competitions;
- services that may be needed by less informed and vulnerable people, e.g., loans to people with a poor credit record, where the aim is to take the revenue from the call rather than to provide the service;
- live chat rooms;
- one-to-one adult chats;
- access to phone-ins run in conjunction with TV programmes;
- donations to charity, especially with celebrities taking live calls;
- the first stage of two-stage dialling for low price international calls;
- dial-up Internet access.

[1] A well-known consumer electronics company used premium rate lines for complaints.

SMS services are commonly used for:

- information services such as sports results and weather;
- voting, often in conjunction with TV programmes;
- games and competitions;
- donations to charity;
- ring tones;
- payments for use of local WiFi access.

Information services and ring tones may be either a single use service or an ongoing subscription service.

With the introduction of live video capabilities on some third generation mobile phones, access to live adult video material is becoming a new application and experiencing fairly rapid growth.

5.1.1 Content issues

Content is regulated or subject to restrictions in some countries. Examples of illegal content or illegal activities that have used premium rate services are:

- gambling;
- prostitution;
- extreme pornography;
- abuse of chat rooms to "groom" minors by adults who often give false descriptions of themselves and try to set up meetings with minors.

These abuses have led to various controls such as regulatory requirements for the recording of chat room conversations and live monitoring of conversations with any offenders being disconnected.

Calls can have their durations extended by the caller being kept on hold or by the live conversation being deliberately inefficient so that the call charge is maximized. In some dating services, callers have been asked during the call to dial additional numbers, which are also premium rate numbers, and all these numbers have been held open for the remainder of the call using a teleconferencing facility, thereby multiplying the call charge several times.

Content issues are not considered further in this supplement.

5.1.2 Misuse by premium rate service providers

The following is a list of the main abuses detected so far:

- Inadequate warning of the tariff. This may be a failure to provide warning required by regulation, or guidelines or licence conditions. Mobile operators are starting to use premium rate SMS to pay for temporary use of WiFi Internet access and may state only that "WiFi roaming charges apply". This is inadequate information as such charges may be very high compared to the charge for a user with a local subscription.
- Callback messages. Messages may be left requesting a callback. The number to callback may be given and a tariff warning omitted, or with mobiles the user may call back without seeing the number being called. This approach is taken frequently for announcing that someone has won a prize or a holiday and they must call a certain number quickly to claim their prize. The number is a premium rate number.

- Services without any normal rate complaint line. The premium rate line may be used for the sale of services or products that are faulty and the caller may have no way to make a complaint and seek a refund or the only way to do so is to call another premium rate number. Problems have been detected with the sale of ring tones where there is an incompatibility between the ring tone and the handset and further downloads are required and charged for without the user having any means to demand a refund.
- Unreasonable extension of the length of calls. The PRSP may organize the answering of the call so that the call duration is maximized by slow answering, putting callers on hold and making conversations unnecessarily long.
- Lack of clarity about subscription services where the subscriber is likely to think that they are buying one-off service and yet they are initiating a subscription service with repeated charging that will continue until they unsubscribe and they may find it difficult to find how to unsubscribe.
- Changing the rate of a call without sufficient in-call warnings. This problem may occur where the billing system is able to support changes of rate during a call, which might be triggered by an option selected by the caller but without sufficient warning about the new rate.
- Call initiation via directory services that by-pass the normal protections such as call barring. This problem could arise where there are directory services that include information about premium rate numbers and allow calls to be connected without the caller re-dialling.
- Access via other high tariff numbers; such as numbers in the mobile range, instead of numbers dedicated to premium rate services. This situation is usually described as revenue share.

5.1.3 Billing cycle misuse

Premium rate services have attracted a number of frauds that exploit the interconnection of premium rate services. The basic scheme is that a fraudster contracts with a terminating operator to provide a premium rate service and then separately subscribes for several lines with an originating operator, normally not the same operator as the terminating operator. The subscriber lines are often at rented premises.

The fraudster then runs autodiallers on the subscriber lines and calls the premium rate numbers continually running up very large bills. The interconnection payments are made monthly and the fraudulent amounts are small in the overall interconnection bills between the operators. The terminating operator makes monthly payments to the PRSP. The subscriber's bills may, however, be 3-monthly and the fraudster continues until a bill arrives or starts to be investigated for non-payment. The fraudster then closes the service and disappears leaving the bills unpaid at the expense of the originating operator who probably has no redress against the terminating operator.

5.1.4 Autodialing viruses (or malware)

This is a variant of the billing cycle abuse that uses the computers of existing subscribers as the callers. The fraudster contracts for a premium rate service and then distributes viruses or other types of programmes through email or web sites that become resident in the computers of legitimate subscribers. If the subscribers have a modem connected to their computer for Internet access, the programmes control the modem to dial the premium rate numbers. Some programmes work during or immediately after an Internet dial-up access session. This runs up high bills that are the responsibility of legitimate subscribers and may not be detected for up to three months. After a period, the PRSP will disappear and repeat the fraud from a new location with a different number and a different identity.

5.1.5 The significance of interconnection

Interconnection, which is an essential part of liberalization and competition at least for normal calls, is the cause of much of the difficulty in controlling abuses. Generous interconnection terms can make the provision of premium rate services highly attractive to new entrants, who do not need a substantial network to provide such services. The established operators are likely to be serving most of the callers and have the problems of handling the complaints about unexpected bills and abuses whereas the terminating operator receives the revenue and avoids the problems. Furthermore, the originating operator does not have any opportunity for introducing controls over the PRSP such as withholding payments for longer than the retail billing cycle or disconnecting the PRSP as soon as an abuse is discovered. The net result is a situation where no party has overall responsibility and the originating operator has not retained enough money to cover any refunds to callers.

Theoretically, the benefit of interconnection and in some cases number portability is that it promotes competition in the hosting of PRSPs. Without it, the providers of PRSPs would need to establish separate connections to each originating operator with a substantial number of subscribers. This would increase their costs, but not too much in those countries where there are only a small number of operators. This approach, however, could work against new entrants, as PRSPs might not bother to establish connection with new entrant originating operators who would then not be able to offer access to their services.

The situation is made much more complex where the 'premium rate' number is in fact an international country code which cannot be readily identified as being 'premium rate'.

5.2 Telephone number misuse

5.2.1 Misuse of international numbers

International country codes as defined in ITU-T Rec. E.164 are intended as addresses to indicate the required destination of a telephone call. When these codes are used in the accounting and settlement procedures, then the accounting rate should be that required for the cost efficient termination of the call in the country designated by the country code. Such codes are not designed to be used as charging band indicators for calls that are terminated short of the designated country. Furthermore separate provision is made within ITU-T Recommendations for designating International Premium Rate and Shared Cost Service.

The use of international country codes usually puts such calls outside any national regulatory provisions on premium rate and revenue share call arrangements.

5.2.2 Misuse inside the country concerned

Some countries, typically very small or developing countries, still have high accounting rates for incoming calls creating a strong incentive for attracting incoming calls. This also applies to countries where some number ranges have different termination rates (e.g., mobile and fixed number ranges). Typically these countries may not have competition in the fixed network. PRSPs arrange to provide services from these countries with the services aimed at callers in distant developed countries and advertise the services in those countries. They negotiate revenue sharing with the local incumbent. The agreement may include the fact that calls to specified number ranges are terminated in a location other than that of the country code country. This creates a pseudo premium rate service that avoids the regulatory controls and consumer protection measures that apply in the developed countries where the numbers are advertised.

The services offered by the PRSP are typically those that are most likely to be accessed by unauthorized calls, especially:

- calls made by younger staff on employers' phones;
- calls made by teenagers without parental consent;
- calls made by auto-diallers.

There is little that can be done to control these abuses from the consumer end. In some cases, operators have considered:

- Handling all calls to the country concerned manually, is passing direct dialled calls to an attendant/operator.
- Selective call screening: These are 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 numbers or country codes towards whom calls are very expensive. Operators may also apply call screening and international numbering block (i.e., CC for networks or geographic areas) or short code barring in the 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).
- Blocking all calls to a country until the abuse is stopped locally.

Both manual intervention and selective call screening are cost-effective and efficient procedures. Obtaining proof of fraud to the degree required by the law is both costly and time consuming. Removing the offending destination from the IDD list reduces the level of loss and puts the burden on others to police the problem and clean up the situation; however, this is an extreme measure and a last resort, but the threat of such action is believed to have prompted actions in the destination country to reduce abuse.

5.2.3 Trading in international minutes and termination

Trading minutes creates the situation where the actual termination of 'international' calls is not obvious. Minutes are traded to an interconnect broker who arranges the onward transmission of the call. Where a country code has been compromised such that valid calls that mature in the specified country are mixed with others that are short stopped for international premium rate services, it becomes very difficult to identify the destination of the short stopped calls. However, all calls are paid for as if they all reach the correct destination. The interconnect broker is unlikely to admit to the actual destination of the short stopped calls and usually falls back on the 'commercial confidentiality' defence. In the circumstance where the short stopped calls are involved in some sort of fraud, it is often difficult to exert any legal pressure, since generally the interconnect broker is in a different country.

5.3 Mobile

Typically, the primary incident at the outset of IRSF fraud is the acquisition of GSM SIMs within the home network. These are obtained by deception, utilizing common methods of identity fraud or document falsification. The complexity of methods is largely dependent on the customer acquisition processes in place. Fraudulent agreements are almost always post-pay or pay monthly in nature. In some cases, SIMs are obtained in large numbers by bogus commercial organizations, in others, connections have been in smaller volumes and are typical consumer subscriptions. The nature of these local customer agreements dictates that the financial losses generated by IRSF fraud are suffered by the home network, because of the complexity and obligations of commercial roaming and interconnect agreements.

Shortly after connection, or after a period dictated by the processes employed by each local operator, the SIM subscribers obtain full international roaming status. SIMs are then shipped to a foreign roaming location – most common foreign destinations (but not exclusively) have been the

networks of Italy, Greece and the United Kingdom. The SIMs begin to generate long duration outgoing international calls. The distinct nature of IRSF dictates that this call traffic appears to terminate in locations that are uncommon within normal usage patterns. The number ranges dialled are, by definition, not premium rate services in the traditional sense. Indeed, the dialled digits will match the listed ITU ranges for known geographical locations. They are, however, not routinely connected with standard voice services and tend to terminate on "audiotext" and other similar products normally associated with traditional revenue share services. It is assumed that despite the nature of international roaming and interconnect charging structures – the termination charges due to the destination international network are subject to revenue share of some sort with the provider of the audiotext service.

The scale of traffic commonly triggers immediate high usage reports from the foreign roaming partner. Whether these are delivered within standard GSMA delivery time-scales or not, significant charges are likely to be incurred prior to action being taken by the home network to suspend the service.

It should be noted that this situation of roaming fraud can exist without abuse of numbering resources.

5.3.1 Viruses in affecting mobiles

This appears to be a new and growing area of fraud but little information is currently available.

Receipt of the viruses may be associated with text or voicemail messages announcing that you have won a prize or there is a special offer available if you call back a special number or just press '9' to reply and confirm details.

There are a number of aspects of this activity which are worthy of note and have become apparent during recent research into international call flows and the various business models in evidence. A number of points can be made:

Existing GSM roaming agreements do not allow for a retention of revenue outside of liabilities under the high usage reporting (HUR) process – any steps taken to enable revenue retention would need to be bilateral.

There is no current framework or governance over international gateways or fixed line interconnect that allows the retention of funds associated with known or suspected fraud.

Any requests made to roaming partners to bar outgoing roaming calls to high risk target regions are dependent on the technological capabilities of the roaming partner and must also be bilaterally agreed.

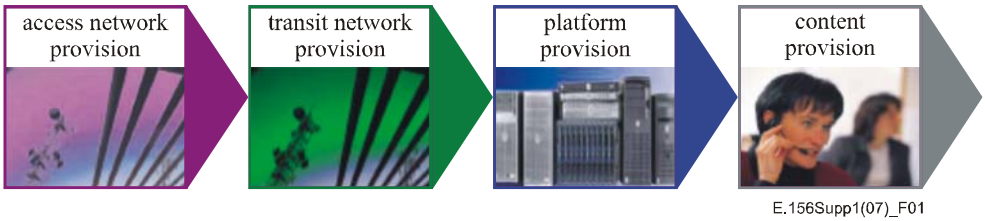
In some cases, it is known that the initial "owners" of a particular geographical number range may no longer have jurisdiction over the deployment of the range and its use. The practice of releasing international number range blocks to third parties has been widespread in the Pacific region. This suggests that short stopping calls, on number ranges disposed of by the original network operator, is common in the IRSF scenario.

Number ranges associated with satellite service providers have also been detected within some case examples.

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.

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 terminating in IRS situations.

The provision of the services behind the situations similar to those related to Internet dumping or web dialers usually involves a wide range of activities and resources, which results in a complex interaction between the involved parties. These relationships take place for the most part in an environment that is more or less invisible or unknown to the end user. Each stage of the value chain has a specific role in the provision of these types of services.



Under the call termination principle, the access network provider is buying a wholesale telecommunications service from the transit network provider. The latter, in turn, is conveying to the content provider via platform provider on behalf of the access network provider. Under the call termination principle, the access network provider therefore is playing the leading part in the value chain with respect to assembling or selling the service to end user. In this situation, the access network provider normally views this type of service as part of its normal revenues and buys call termination services for information services in the same way as he buys termination services for international calls.

6 Best practice to counter misuse

6.1 Introduction

This clause outlines the activities that can be taken to minimize the impact of misuse, and it is recognized that describing best practice counter misuse can be described in various ways, and no one way is better than the other. However for the purposes of this Guide, it is recognized that best practice can be associated with the various industry stakeholders, e.g., Regulators, Recognized Operating Agency, or associated with the various relationships that exist, for example between recognized Operating Agencies or between ROAs and SPs or consumers.

The best practice will be presented in the following way:

- Regulatory
- Recognized Operating Agency
  - Consumer;
  - Commercial;
  - Technical.

6.2 Background

The main consumer problem with premium rate services is that the subscriber receives an unexpectedly high bill. There are five possible causes:

- The subscriber was unaware of the tariff that applied to the call.
- The subscriber was unaware that they can have premium rate calls barred or thought that a call bar applied when it did not.

- The call was made by another individual and was not authorized by the subscriber (the caller may have been unaware of the tariff or may have deliberately stolen the call).
- The call was made automatically by a computer activated, for example, by a virus without the subscriber being aware of what was happening.
- The subscriber is not aware of the nature of the service, for example they think that they are buying one-off service and yet they are initiating a subscription service with repeated charging that will continue until they unsubscribe.

In all these cases, the problem can continue for the whole of a billing period or longer before being detected. Unless there are special measures, the problem is unlikely to be detected by the subscriber before the next bill arrives. Detection can take even longer if the subscriber pays by direct debit and does not check their bills carefully.

Billing practice varies widely from operator to operator; some use monthly billing cycles and other use up to three months. In some cases, there is a delay of several weeks while the bill is being prepared.

Pre-payment systems provide some protection, as with unexpectedly high usage the payment would be exhausted unexpectedly quickly and so trigger an investigation provided the service provider does not allow negative credit to accumulate without the subscriber's knowledge. Some service providers are allowing negative credit of at least 20 Euros such that when the subscriber tops up their credit with say a 10-Euro voucher, the voucher is used up immediately.

Many operators provide itemized billing and this helps users to investigate the cause.

The unexpected bills lead to complaints that can be hard to resolve. Some complainants claim that there has been a genuine billing error and that the calls were never made, and it can be difficult or impossible to determine objectively who made a given call or if the call was actually made from the account claimed.

A more minor problem is misdialling, i.e., dialling a premium rate number by accident when meaning to dial a normal rate number. This can be expensive if the number triggers a one-off payment.

The power of premium rate debt over consumers is greatly increased if the originating operator is entitled to suspend the service because of non-payment of the bill and if there is no alternative access provider. If the PRSP had to use the normal legal processes for debt recovery, it would not be cost effective to recover the smaller debts and the PRSP would not be willing to go to Court in cases where it had not complied with all relevant legislation.

Consumer protection measures differ widely from country to country and may be a combination of:

- codes of practice;
- guidelines;
- contractual conditions imposed by operators on PRSPs.

The enforcement capabilities may well also vary widely and may include disconnection, fines and criminal prosecution. In some cases the fines may be "voluntary", i.e., not supported by legislation and not ultimately enforceable. Voluntary consumer codes and measures may work with reputable PRSPs but are ineffective with ones who are prepared to operate outside the law. Experience has shown that the money that can be made with premium rate services is sufficient to attract various criminal elements.

Legal measures and enforcement are normally applied only on a national basis and can be avoided if services are offered from one country to another. Cross border enforcement has not been developed much to date.

The following clauses describe the various consumer protection measures that are used in different countries and some that are new ideas. Most countries use a combination of measures.

The consumer protection measures for abuses of international numbers are more limited because the numbers are not easily distinguished from normal numbers in other countries and therefore the originating operator is normally not in a position to apply any of the measures that they would apply for national premium rate numbers.

Generally any measure that increases the subscriber's awareness of the current level of their bill will help to prevent repeated problems for the same subscriber. Hence arrangements such as notification of unusual increases in a bill, and limits on the spend or duration of an individual call, will all help.

NOTE – This clause does not apply to the possible introduction of cross border premium rate services, which is outside the scope of this supplement.

6.3 Regulatory

6.3.1 Limitations in the types of services that may be offered

Various types of services may be prohibited.

6.3.2 Organization of the numbering ranges used

Most regulators require premium rate services to use a specific numbering range so that consumers can learn to distinguish premium rate numbers and so that call barring can be applied using simple algorithms.

Different sub-ranges may be used for different types of premium rate service, e.g., to distinguish business and entertainment services.

National authorities should be encouraged to state their positions on "notoriously abused" destinations (e.g., 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 recognized as being misused.

6.3.3 Registration of PRSPs and identity checks on staff at PRSPs

Registration would make it easier for the regulator to investigate complaints and for consumers to contact the PRSP themselves.

Identity checks on senior staff and directors would be aimed at reducing fraud and making it more difficult for fraudsters to repeat frauds using different companies.

6.4 Recognized Operating Agency

6.4.1 Consumer

6.4.1.1 Price warnings

Many countries require advertisements of premium rate services to include the price and to do so with a specified form of words and/or print of at least a given size. However, such warnings are only effective in a limited number of cases as not all are advertised (in particular data services) and even when they are advertised, there is only little chance that a consumer knows or remembers the content of such advertisements when he seeks access to these services.

Price warnings and information on the number used that are provided just before access is established are more effective in this respect. There are various parties involved that may be technically capable of providing this information, including the originating operator, the terminating

---

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

operator and also the content provider. Some countries require a price-warning announcement to be played without charge for audio services at the start of each premium rate call. The terminating operator usually provides the warning itself, but the terminating operator may not be aware of the exact retail price paid by the caller, which depends on the originating operator.

For data services accessed by web diallers, the possibility exists to provide tariff and number information by means of software to be installed on the end-user's PC that is able to detect outgoing calls via the analogue modem of the PC.

The responsibility for price and tariff transparency may be placed jointly on the originating operator (as this party bills for the services) and the content provider. The actual implementation may be carried out by only one of these parties.

Some countries separate the charge paid to the PRSP from the charge paid for the communications and require warnings over the charge paid to the PRSP, which can be given at the terminating end, whilst leaving the charge for the communications to be more competitive but less transparent. This gives flexibility for different communications charges between fixed and mobile operators.

6.4.1.2 Itemized billing

A requirement can be imposed for all calls to premium rate numbers to be itemized even if the caller has not subscribed to itemized billing for normal calls. This measure does not protect, however, against the first occurrences of high bills due to unawareness of the risks associated with premium rate numbers.

6.4.1.3 Right to a refund for the first high bill

This is a protection against the first occurrence of a high bill. The subscriber is given a right to a refund unless it can be proved that the subscriber was aware that premium rate calls were being made on their account. The aim is to provide an opportunity for the subscriber to become aware of the risks and to request call barring or other protections.

This protection, however, raises the question of who should provide the refund. One regulator places this requirement on the PRSP because they are the party who has collected the main part of the revenue and who may have designed the service to attract unauthorized calls. The originating operator in contrast is the party whom the subscriber can most easily contact and complain to. Furthermore there is a risk that the PRSP will go out of business before paying refunds if there are many demands for refunds. There is also an issue of whether the refunds can be enforced legally or depend on the voluntary cooperation of the PRSP.

In order to provide more security for refunds, some regulator require PRSPs to deposit bonds of several thousand Euros before starting to offer services so that these funds can be used for refunds if needed.

6.4.1.4 Credit limits and warnings when specified levels are exceeded

Operators could be required to limit the spend on premium rate services in each billing period. This limit could be set by the regulator, the operator, or the subscriber. For example, one country requires a system where there needs to be opt-in after the bill increases by 10 Euros.

An alternative is to require the operator to notify the subscriber when a limit is reached and optionally to require specific authorization if the limit is to be increased.

6.4.1.5 Barring of specific numbers

Operators with international connections need to be able to bar calls to specific foreign numbers where there is evidence that they are involved in abuse or fraud.

6.4.2 Commercial

6.4.2.1 Delays in payments to PRSPs

This protection is aimed at reducing fraud. Originating or terminating operators would be required to delay interconnection payments or payments to PRSPs by at least one complete retail billing cycle. This would provide time for abuses to be detected before the money is passed to the PRSP. Withholding of payments by the originating operator would give them more effective control and enable them to use the money for refunds.

There are two approaches to address these problems:

- To empower the originating operator to handle complaints and give refunds and to withhold payments to the terminating operator to cover possible repayments or to have arrangements for obtaining refunds from the terminating operator.
- To arrange for independent complaint handling and refunds from the PRSPs.

The first approach is simpler and requires less involvement of the regulator, whereas the second is more complex and difficult to implement effectively.

6.4.2.2 Termination of premium rate calls within the country

This requirement is that all calls to premium rate numbers must be terminated in the same country as the originating network. The aim is to ensure that the PRSP is under the same regulatory and legal regime as the callers. This approach, however, may conflict with obligations within the EU to allow cross border services.

6.4.2.3 Limiting interconnection

As explained earlier, interconnection increases the scope for abuses and the resources needed for regulation. A measure that did not allow calls to higher risk numbers to pass across interconnection points would mean that for such calls the originating and terminating operators would be the same and could carry out their own consumer protection measures. Carrier selection operators would not be allowed to carry such calls. This measure would reduce the workload for regulators in handling complaints, but it would mean that PRSPs who serve such numbers would have to establish multiple connections for call termination. In consequence, it would disadvantage new entrant originating operators as they would not generate sufficient calls initially to justify a connection and so would not be able to provide access to the new services. As such the measure would restrict competition by increasing the barrier to market entry for a new operator.

6.4.2.4 Complaint organizations run by or for PRSPs

PRSPs could themselves establish and fund a common complaint-handling organization as a system of "self regulation". This would need publicity so that subscribers would know whom to contact.

As the financial damage to individual consumers is in many cases too low for it to be worth their taking legal action, such complaint organizations would improve their position significantly. A limitation, however, is that such arrangements would only deal with national numbers.

It is known that in at least one European country there is strong support from the content providers for a legal requirement for PRSPs to join such an organization.

An example of a similar organization is the GSMA Fraud Forum (GSMA-FF) that has established a relationship with the Pacific Islands Telecommunications Association (PITA) and highlighted the use of Pacific island number ranges in fraud incidents. PITA has expressed serious concern at the impact this fraud is having on the reputation of the Pacific Islands and has developed an action plan to respond. GSMA-FF will assist PITA in developing a code of practice amongst members on audiotext and other high risk services.

6.4.3 Technical

6.4.3.1 Call barring or opt-out

Many regulators require operators to offer to subscribers call barring to premium rate numbers. To be effective, subscribers need to know to consider whether or not to have call barring applied. Efforts such as advertising are needed to promote this awareness amongst consumers especially if new service types in the premium rate market are opened up.

Call barring can be rendered ineffective if it is required only of the operator who provides the physical access line and carrier pre-selection is used or carrier selection with a smart box to add the selection code automatically. Unless the call barring applies to all calls, the use of carrier (pre)-selection may by-pass the barring. Usually the subscriber will be unaware of this weakness. Call barring needs to be provided by all operators who may be selected by the subscriber.

Selective call barring by a network operator may prove effective against numbering frauds, as the customers cannot 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.

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

6.4.3.2 Faster billing

Some of the fraud problems arise because the operators use a longer billing period for retail services than for interconnection. The fraud risks would be reduced if the retail billing period were reduced to be no longer than the period for interconnection billing.

6.4.3.3 Traffic monitoring

Frauds such as autodiallers and billing cycle abuse generate sudden increases in traffic. Routine monitoring of traffic levels by operators should be able to detect such abuses and routine monitoring of subscriber call records could detect potentially unauthorized calls. Where operators are able to communicate with subscribers by email or automated calls or leaving messages in network-based message systems, they could easily advise the subscriber of the potential problems. This approach could cause problems concerning data protection at least as far as individuals are concerned.

6.4.3.4 Requirements on auto-dialling software

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 user's 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.

Internet "dumping" or modem hijacking takes place when, unknown to the user, an Internet dialler transfers the user from the current Internet service provider (ISP), which is usually accessed using an un-timed local call, to a different telephone number usually associated with high termination rates (e.g., Number ranges that have revenue share associated with them (premium rate services (PRS), international revenue share (IRS), or mobile terminations in some destinations)).

The users are unaware that this has happened until they receive their next telephone bill. Internet dumping is more likely to happen through adult content sites and sometimes appears associated to misuse of numbering plans.

Worldwide operators have received many complaints about Internet dumping. Internet users have found that, while they surfed the net or went to non-adult sites, diallers had downloaded themselves, or the user, who may have thought it was some other piece of software, inadvertently downloaded them.

It should be noted that not all diallers are rogue ones and involved in Internet dumping fraud. Some diallers are used to commercial and security issues and, consequently, it is important to distinguish among diallers which are the rogue ones.

The problem of PC diallers has been addressed in different ways. Some countries, such as Germany, have passed specific regulations to make it illegal to download PC diallers without user consent. Austria has in addition implemented the opt-in principle for PC diallers. The list of countries that have adopted special regulations on PC diallers also includes Belgium, the Czech Republic, Finland, Spain and the UK. Other countries have not seen such legal measures as necessary, but have instead relied on preventive action taken by the access operators on the basis of existing legislation against fraud. In November 2004, Ireland lifted an obligation it had previously placed on Internet service providers because it concluded that they were now able to provide the necessary consumer protection without it.

It is recommended that National Regulatory Bodies take pro-active action standardizing the diallers to be used. This way it will be easy to clearly distinguish between a rogue and a normal dialler. It must be noted that the use of diallers is most of time associated with calls associated with Number Resources that have an element of revenue share associated with them, which use and access is regulated by the National Regulatory Bodies.

It is recommended that, with respect to fraud, only rogue diallers, mainly those producing Internet dumping and/or modem hijacking, should be blocked.

It is also recommended that operators should prepare their fraud staff to new situations such as web diallers. This needs to be done involving CRM staff as well.

A methodology to detect rogue diallers and identify the scheme used for that telecommunications fraud was developed and involves some "hacking methodologies" such as the use of sniffers (with the possibility to decode packets) and reverse engineering programs. It was concluded that operators should prepare their fraud staff concerning new situations such as web diallers, being able to discriminate between (normal) diallers and rogue-diallers (modem hijacking). This needs to be done involving customer relations management (CRM) staff as well.

This would require all auto-dialling software used with premium rate numbers to contain a warning about the charge rate in sufficiently large print, which has to be explicitly accepted by the user, and would require registration of all such software. PRSPs would not be allowed to collect money for calls from software that did not carry an appropriate signature from the registration process. Germany, for example, requires certain minimum requirements for the auto-dialling software and registration of each individual copy of the software, which receives a unique signature, and their scheme involves opt-in through explicit acceptance by the user of the call charges.

6.4.3.5 Constraints on CLI presentation

A protection that would reduce abuse of mobile subscriber through automated callbacks, especially on SMS, would be for the mobile operators to inhibit the presentation of any CLI that is a premium rate number, thus a legitimate caller would need to leave the number within the message and so the called subscriber would be more likely to see that the number is premium rate.

6.4.3.6 Intelligent barring of specific numbers

One incumbent fixed operator has introduced a system of intelligent traffic filtering that has proved to be highly successful against fraud that arises from auto-diallers. Whenever a call to Internet dial-up access number is terminated and an outgoing international call with the nature of the call indicator set to "data" is established within 15 seconds, then the called international number is identified as a potential number for fraudulent calls and all calls to that number are blocked for a period of a month, unless the operator receives other information to the effect that the number is legitimate.

6.4.3.7 Traffic analysis

Traffic analysis should facilitate identification of calls to international numbers that are being used as pseudo premium rate numbers or are subject to short stopping. Unexpectedly high levels of traffic and sudden changes in the level of traffic are indicators of potential problems.

Where these practices occur, at least one operator is cooperating in the arrangement. Operators will normally respond to complaints once the practice is identified or if not to threats to block all their traffic. The problem is that blocking all traffic will prevent some legitimate calls being made.

Operators 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 the 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 should 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.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	**Overall network operation, telephone service, service operation and human factors**
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2008