Body of European Regulators for Electronic Communications

BEREC

BoR (10) 62 Rev1

BEREC report on cross-border issues under Article 28(2) USD

February 2011

Table of Contents

Executive summary

As end-users begin to use services provided in Community Member States (MS) other than their own, their protection in relation to those services presents new challenges.

So far this phenomenon has been relatively limited in scope. The new version of Article 28 of the Universal Service Directive (USD), Directive 2002/22/EC (the 2002 USD), reviewed by Directive 2009/136/EC (the 2009 USD), to be transposed into national legislation by 25th of May 2011, provides that, where technically and economically feasible and except where a called subscriber has chosen for commercial reasons to limit access by calling parties located in specific geographical areas, end-users in one MS should be able to access any number within the Community; this extends the type of number and service to which access shall be given, but maintains the same conditions as under the 2002 USD.

The same Article also anticipates that end-users may become the victims of fraud or misuse (including misuse of numbering resources). The text requires MS to ensure that the relevant authorities, which may be the National Regulatory Authorities (NRAs) and/or other designated authorities, are able to require undertakings providing public communications networks and/or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require that, in such cases, providers of electronic communications services withhold interconnection or other service revenues. Regulation (EC) 1211/2009 establishing BEREC also provides that it is a task of BEREC, on request, to provide assistance to NRAs on issues relating to fraud or the misuse of numbering resources within the Community, in particular for cross-border services.

Therefore, following the recommendations arising from previous work done by ERG, BEREC surveyed NRAs with the aim of:

- Identifying situations where cross-border issues arise, or are expected to arise in the future, including possible forms of fraud as well as cases of breach of regulatory obligations that could fall within the scope of paragraph 2 of Article 28 USD [(1)];

- Understanding how NRAs are currently handling those issues and which instruments they have in place to address them;

- Understanding what practical challenges are likely to be faced by NRAs in the event that they are designated as a relevant national authority with powers under Article 28(2) USD in cross-border cases.

Overall, 22 NRAs responded to the questionnaire, including 20 European Union (EU) MS and 2 European Free Trade Association (EFTA) MS [(2)].

Given that the transposition process was still underway in MS, generally NRAs were not yet able to provide detailed views on this matter.

To provide further input, BEREC conducted additional research, in particular on: the technical aspects of blocking access to numbers/services and withholding interconnection revenues; the functioning of existing cross-border cooperation mechanisms and the 2006 recommendations of the European Conference of Postal and Telecommunications Administrations (CEPT) and the International Telecommunication Union (ITU) in relation to cross-border misuse of numbering resources; and the scope of NRAs' current competencies regarding premium rate services (PRS) regulation and the relationship between such powers and NRAs' expectations about the "relevant authorities" likely to be designated in its MS.

---

(1) International roaming is not felt to pose cross-border challenges to be considered in this context.
(2) **NRAs from the following 22 countries responded to the questionnaire**:
20 EU countries – Belgium, Czech Republic, Denmark, France, Finland, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Sweden, United Kingdom (UK);
2 EFTA countries – Norway and Switzerland.

The report also takes account of comments received in response to the stakeholder consultation launched between 9th December 2010 and 13th January 2011 on a draft version of this report.

It is important to note that while reflecting the views expressed by NRAs in their answers to the questionnaire, this report is not intended to make an assessment of the different national approaches to cross-border issues. They should be considered within the context of the national market's characteristics and, in particular, of national legislation, which in some cases gives relevant competencies to national authorities other than the NRA.

In light of the latest legislative developments at EU level and considering the information collected from NRAs, the purposes of this report are to explore:

a) The extent to which cross-border instances of fraud or misuse within the scope of Article 28 of the USD might arise in the future and what number ranges and services might be affected;

b) Current national conditions and practices in respect of cross-border issues, as well as to anticipate if or how they might change due to the transposition into national legislation of Article 28 of the USD, in particular paragraph 2;

c) How the enforcement powers of requiring networks and/or providers to block access to numbers/services and withhold interconnection revenues may work in practice in regulatory and technical terms, both on a domestic basis and where the numbers have been allocated by another MS and/or the service originates in another MS;

d) Areas where it may be appropriate for BEREC members to cooperate and the form that such cooperation might usefully take, with reference to existing cooperation mechanisms and previous CEPT and ITU recommendations;

e) Areas where further work is needed, presenting proposals accordingly.

Structure of the report

The report is divided into 5 sections:

a) Section 1 introduces the paper, its background and the possible challenges arising from the revised USD;

b) Section 2 gives an overview of cross-border issues that are being considered by NRAs as included within the scope of Article 28(2) USD and that have arisen in the past or the present, or that are likely to arise in the future. Also, it aims to give an overview of the practices implemented by NRAs handling those cases, of other existing national bodies with competencies on this matter, as well as of relevant international cooperation mechanisms currently operating and previous recommendations from the CEPT and ITU;

c) Section 3 reflects how NRAs anticipate Article 28(2) USD to operate in practice, specifically what measures or procedures they consider important to have in place to allow NRAs to effectively use that provision where they are a “relevant national authority”, and to work with other relevant authorities that are not NRAs;

d) Section 4 identifies areas where further work is needed, including cross-border cooperation, and presents proposals accordingly.

1. Introduction

1.1. Background of Article 28 of the USD

In its original version, the USD already covered cross-border issues in a specific way, particularly access to non-geographic numbering resources across the Community. Former Recital 38 stated:

"*Access by end-users to all numbering resources in the Community is a vital pre-condition for a single market. It should include freephone, premium rate, and other non-geographic numbers, except where the called subscriber has chosen, for commercial reasons, to limit access from certain geographical areas. Tariffs charged to parties calling from outside the Member State concerned need not to be the same as for those parties calling from inside that Member State.*"

Also, in former Article 28 "Non-geographic numbers", the USD stated that:

"*Member States shall ensure that end-users from other Member States are able to access non-geographic numbers within their territory where technically and economically feasible, except where a called subscriber has chosen for commercial reasons to limit access by calling parties located in specific geographical areas*".

The 2007 proposal of the European Commission (EC) for a Directive of the European Parliament and of the Council amending the USD aimed to adapt the regulatory framework by "*strengthening certain consumers' and users' rights (in particular with a view to improving accessibility and promoting an inclusive Information Society), and ensuring that electronic communications are trustworthy, secure and reliable and provide a high level of protection for individuals' privacy and personal data"*. The EC's 2006 report to the Parliament and the Council on the functioning of the regulatory framework had previously noted that "*there was room for improvement in the field of consumer protection and security to ensure that* [the framework] *kept pace with technological developments and remained effective for the coming decade*".

In light of these aims, the EC proposed considerable changes to several provisions of the USD, including Article 28. It proposed to extend the scope of Article 28 in terms of the services covered, specific references to the role of NRAs, and enforcement in the case of fraud or misuse, as follows:

"Member States shall ensure that national regulatory authorities take all necessary steps to ensure that:
(a) end-users are able to access and use services, including information society services, provided within the Community; and
(b) end-users are able to access all numbers provided in the Community, including those in the national numbering plans of Member States, those from the European Telephone Numbering Space and Universal International Freephone Numbers.
National regulatory authorities shall be able to block on a case-by-case basis access to numbers or services where this is justified by reasons of fraud or misuse."

The EC considered that its proposed wording fostered *"access to cross-border services, thereby contributing to the completion of the Internal Market for citizens and business*".

In its draft Report on the EC's proposal, the European Parliament proposed an amendment to enable NRAs to ensure that, in case of fraud and misuse, electronic communications providers withhold relevant interconnection revenues, in addition to blocking access to numbers or services. The Parliament considered that the measure most likely to effectively block fraud and misuse is the withholding of revenues.

After a long debate at EU level, the Framework Review package was adopted in November 2009. It specifically discusses cross-border issues in Recital 46 of the Citizens' Rights Directive (2009/136/EC):

"*A single market implies that end-users are able to access all numbers included in the national numbering plans of other Member States and to access services using non-geographic numbers within the Community, including, among others, freephone and premium rate numbers. (…) Cross-border access to numbering resources and associated services should not be prevented, except in objectively justified cases, for example to*

combat fraud or abuse (e.g. in connection with certain premium-rate services), when the number is defined as having a national scope only (e.g. a national short code) or when it is technically or economically unfeasible. Users should be fully informed in advance and in a clear manner of any charges applicable to freephone numbers, such as international call charges for numbers accessible through standard international dialling codes."

Accordingly, the new version of Article 28 "Access to numbers and services" now establishes that:

"*1. Member States shall ensure that, where technically and economically feasible, and except where a called subscriber has chosen for commercial reasons to limit access by calling parties located in specific geographical areas, relevant national authorities take all necessary steps to ensure that end-users are able to:*

a. *access and use services using non-geographic numbers within the Community; and*
b. *access all numbers provided in the Community, regardless of the technology and devices used by the operator, including those in the national numbering plans of Member States, those from the ETNS and Universal International Freephone Numbers (UIFN).*

(…)."

The Citizens' Rights Directive also introduced paragraph 2 to Article 28, which established enforcement powers in relation to access to numbers or services where this is justified by fraud or misuse, including on a cross-border basis.

Accordingly, "*Member States shall ensure that the relevant authorities are able to require undertakings providing public communications networks and/or publicly available electronic communications services to block, on a case-by-case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues.*"

As a starting point, a key feature of the new Regulatory Framework reflected in the revised Article 28 of the USD seems to be the growing role of national authorities, which may include NRAs, in addressing consumer protection issues that transcend national borders, as well as

an increasing space for coordination between regulatory authorities, where the relevant numbers and services may be accessed cross-border.

The NRA's ability to address problems that transcend national borders appears to be particularly important for applying specific enforcement actions, pursuant to paragraph 2 of Article 28 USD. Under such provision, all "relevant authorities", which might be electronic communications regulatory authorities or others, such as consumer protection authorities, should be empowered by existing national legislation or legislation to be created at a national level within the current transposition process. Such legal empowerment shall allow them to require providers of public communications networks and/or publicly available electronic communications services to:

- **Block, on a case-by-case basis, access to numbers or services where this is justified by fraud or misuse**, and
- Require that, in such cases, providers of electronic communication services **withhold related interconnection or other service revenues.**

The Citizens' Rights Directive does not provide a definition of "fraud" or of "misuse", the two situations that may justify those enforcement actions to be taken.

1.2. Challenges arising from the revised USD

According to the third edition of the **Consumer Markets Scoreboard**, published last March by the EC, EU consumers are still not reaping the full benefits of the internal market, namely the possibility of a wide choice, due to barriers to cross-border commerce of products and services, some of them of a structural nature such as language, consumers' preference for national suppliers or consumer protection law, others linked to the current economic climate, contributing to a decline in consumer confidence.

With that in mind, the Scoreboard concludes that sustained efforts are needed across Europe and in all economic sectors to improve quality of regulation concerning consumers and businesses, effectiveness of resolving disputes and handling complaints, and consumer trust in authorities, providers, advertisers and consumer organisations.

Concerning the electronic communications sector, BEREC considers that the implementation of the revised USD, by giving end-users the ability to access and use, where technically and economically feasible, services using non-geographic numbers within the Community, as well as accessing all numbers provided in the Community, may contribute to EU internal market to be more integrated and to enhance end-users' awareness of cross-border opportunities. It may also contribute to end-users in general not being treated differently on grounds of their nationality or place of residence.

However, where such cross-border provision is technically and commercially feasible, increasing the efficiency of cross-border enforcement will also be important. The EU legislator understands this and, by introducing paragraph 2 to Article 28 of the USD, therefore is giving MS a signal that particular number ranges and services cannot operate, in the event that they are linked to fraud and misuse, which requires enforcement actions by the relevant authorities, by requiring networks and/or providers to block access to numbers/services or withhold interconnection or other service revenues.

Consumer harm may that way be reduced or prevented, which will contribute to increasing the level of confidence that end-users have in cross-border commerce of services.

Nonetheless, the implementation of the revised Article 28 of the USD poses clear practical challenges.

The first one is the possible need to define cooperation procedures between NRAs so as to facilitate cross-border enforcement. Moreover, in some countries, a different national body may be designated as a relevant authority in addition to or instead of the NRA, making cooperation more complex.

Secondly, another practical challenge is that “fraud” and “misuse” are not defined by the USD and may have different definitions in different countries. It is therefore possible that, for example, the NRA in one country will not be able to act on a complaint made by the NRA in another country, on the basis that it does not find that the alleged misdeeds constitute “fraud” or “misuse” under its national definitions.

There are relevant international recommendations on the meaning of “misuse” in relation to numbering resources, which may be considered in this context, as follows.

Specific to international numbers, in its 2006 Recommendation on “*Consumer Protection in case of Misuse or Unauthorised Use of International E.164 Numbering Resources*”, which expressed particular concern about Internet diallers, the Electronic Communications Committee (ECC) within the CEPT provided that *“misuse should be understood as the use of international E.164 numbering resources:*

i. *non effectively assigned, often within CC* [country code] *without the knowledge of the assignee (or number resource holder); or*
ii. *to initiate calls that do not terminate in the country or network of the number resource holder, except in cases where the end-user invokes the call forwarding functionality; or*
iii. *for purposes other those for which they were assigned”*.

When evaluating this possible definition, it might be necessary to further consider and specify the meaning of “non-effectively assigned”.

Also, the 2006 ITU-T Recommendation E.156 “*Guidelines for ITU Action on Reported Misuse of E.164 Number Resources*” provides that:

“A misuse of an E.164 international numbering resource occurs where the use of that numbering resource does not conform to the relevant ITU-T Recommendation(s) assignment criteria for which it was assigned or when an unassigned numbering resource is used in the provision of a telecommunications service”.

Meanwhile, “fraud” or certain aspects of “fraud” are likely to be considered a criminal offence in some countries, falling within the competencies of the criminal enforcement authorities. In some cases, communications providers themselves may take action to block access to international numbers where they consider there is a significant risk of fraud, as in such cases providing cross-border access is not “economically feasible”.

In any case, purely for the purposes of completing the NRA questionnaire to inform this report, and without prejudice to each MS's own definition, NRAs were asked to give the expressions "**Fraud**" and "**Misuse of numbering resources**" the following meaning:

- "**Fraud**: *any deceitful practice with cross-border impact perpetrated for profit or to gain some unfair or dishonest advantage over end-users of electronic communications services"*;

- "**Misuse of numbering resources**: *use of numbering resources in an unauthorised way, which may cause harm to end-users of electronic communications services and with cross-border impact*".

Thirdly, at present there seem to be some differences in the ways NRAs may deal with blocking the access to numbers, where they are a relevant authority. In general terms, while some NRAs have powers to require access to numbers to be blocked, others for instance appeal for cooperation from network operators so that they block access to numbers in a voluntary basis. Some NRAs envisage that they will need a modification in national legislation in order to be able to establish an effective blocking of numbers.

Last, in response to the public consultation, one of the stakeholders [(3)] has drawn attention for other possible challenge arising from the implementation of the revised Article 28 of the USD: in the event that an "open access" approach to numbers and services was adopted in accordance with Recital 46 of the Citizen's Rights Directive (2009/136/EC), amending the USD, and, mostly, Article 28(1) USD, this would increase the likelihood of fraud and misuse, requiring coordinated action among different NRAs.

[(3)] European Telecommunications Network Operators' Association (ETNO). It was established in May 1992 as policy group for European electronic communications network operators with the purpose of enabling discussion between its member companies and decision-makers for the development of the European Information Society.

1.3. Previous work by ERG on cross-border enforcement

Cross-border enforcement was already addressed in previous work done by ERG under the End-Users Project Team.

This initial work, mainly focused on cross-border consumer issues, did not seek to identify an exhaustive list of consumer protection issues raised by cross-border services, or to identify solutions to them all. Rather, it sought to consider what those issues might be, in particular in relation to VoIP and numbering, and how they might be handled in practice.

In general terms, it was found that cross-border consumer enforcement issues may arise where a user of a numbering resource in one state commits fraud or misuses that numbering resource to the detriment of a consumer calling that number from another state.

To date, most complaints of this nature, usually about PRS numbers, are national (i.e. the PRS provider and consumer are in the same country). This may be for various reasons:

- PRS content, if any, is typically national;
- In some countries, PRS providers do not make money if a call is made from outside the country, because international carriers do not provide repayment services to PRS providers; and
- In some cases, to date it is not possible to access a PRS number from outside the country. Paragraph 1 of Article 28 of the revised USD might affect this, although it still contains the conditions of technical and economic feasibility, as in the 2002 USD.

PRS and related anti-fraud initiatives are in place in several countries, but these focus mostly on national scams. However, there is already some anecdotal evidence of this kind of consumer harm occurring on a cross-border basis. Also, cases like this might increase in the future, potentially as a result of the new version of Article 28 of the USD, which intends (subject to some caveats including economic and technical feasibility) to enable end-users to access all numbers and services within the Community. This leads BEREC to consider how the new enforcement powers of relevant authorities under the revised Article 28 of the USD could be used in practice.

Because some NRAs already seem to have experience in dealing with cross-border issues at a national level, lessons can be learned from this experience, as well as from other national regulatory bodies responsible for PRS in a given MS. With regard to cooperation mechanisms that are being developed to address these issues in full or in part, further consideration of the work of the IARN could be warranted.

Therefore, the previous work done by ERG recommended collating and analysing complaints data from NRAs to try to identify any emerging cross-border issues that might merit special attention. Furthermore, it also recommended research into the nature and scope of any specific cooperation arrangements and other initiatives, which already exist.

2. Current practices

Drawing on the BEREC questionnaire completed by NRAs in May – June 2010, this section gives an overview of cross-border issues that NRAs considered may fall within the scope of Article 28(2) USD and that had arisen in the past or the present, or that seemed likely to arise in the future.

Also, it aims to give an overview of the practices implemented by NRAs handling those cases, of other national bodies with competencies in this area, as well as of relevant international cooperation mechanisms currently in operation.

2.1. Overview of current services and associated number ranges possibly within the scope of Article 28(2) USD

NRAs identified various numbers and services currently in use that could fall within the scope of Article 28(2) of the revised USD, in the event that they are subject to fraud or misuse.

In some cases, NRAs also gave an assessment of the likelihood that a particular number range or service might be subject to fraud or misuse in the future, which could make developing a cross-border cooperation mechanism especially relevant.

The common characteristic of the services and numbers mentioned by the respondent NRAs is that they cost more than a standard geographic or mobile call, SMS or MMS. They include “revenue share” numbers and services, including premium rate, as well as international, satellite and VoIP numbers and services.

With the exception of Internet diallers, where NRAs expected cases of fraud or misuse to decrease as end-users move away from dial up Internet to broadband connections, regulators in general terms felt that fraud and misuse would remain a risk in the future. In particular, they noted that if greater cross-border access is given to premium rate numbers and services through transposition of Article 28(1) of the USD, problems of cross-border fraud and misuse would be likely to increase. NRAs also felt that fraud and misuse of VoIP

numbers and services may grow in so far as general take-up is growing. The Danish NRA, NITA, noted that most queries about jurisdiction and enforcement for cross-border service provision came from VoIP providers, and that it is increasingly necessary for such questions to be clarified.

2.1.1 Examples of fraud or misuse related to revenue share numbers or services, including premium rate

The services and number ranges cited most frequently by regulators were PRS (fixed and mobile, including voice, SMS and MMS). The majority of respondent NRAs [(4)] identified premium rate numbers or services as potentially falling within the scope of Article 28(2) of the USD. Seven of these specified that they expected fraud or misuse of such numbers or services to continue or increase in the future, including on a cross-border basis [(5)]. In the next couple of paragraphs we will briefly explore how PRS work, to understand the scope for instances of fraud or misuse.

To use premium rate numbers or services, end-users may contact such numbers themselves, or agree to receive messages. They can be accessed and delivered over a range of platforms – fixed voice and Internet; mobile voice, SMS and mobile Internet; and interactive digital television – which are increasingly converging. In response to the public consultation, one of the stakeholders [(6)] pointed out that NRAs should consider differentiating between PRS generally, and directory services, "the latter being electronic communications services providers and hence already complying with authorization requirements".

Although the end-user receives a single bill from the electronic communications service provider, the service has two parts – an electronic communications service and a content service. These are typically provided by different parties, where the provider of the revenue

[(4)] NRAs from Belgium, Czech Republic, Finland, France, Greece, Ireland, Malta, Netherlands, Poland, Sweden, Switzerland and UK.
[(5)] NRAs from Belgium, Germany, Greece, Netherlands, Slovak Republic, Sweden and UK.
[(6)] The Number and its group companies are worldwide providers of directory enquiry services. In Europe they perform in the UK, France, Italy, Austria, Switzerland and Ireland.

share service is separate from the electronic communications provider, and might contract out the provision and/or promotion of the service to a further party (the content provider). Alternatively, they may be provided by the same party, particularly a mobile provider offering downloads from its own web portal, which is regulated as a PRS in some, but not all, countries.

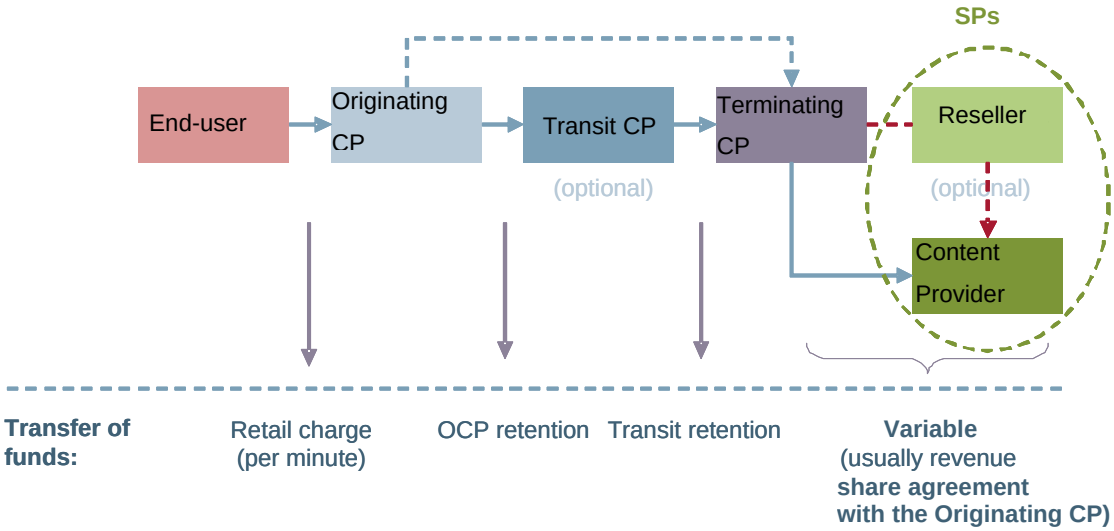
As such, these numbers and services offer a micro-payments system. Regulators generally hold the service provider responsible for all aspects of the revenue share service (although in some cases, they may consider holding the content provider responsible, where this is a different party). As regards the content, 'digital' goods and services are most common at present, and include information services like financial information or news and weather; customer services from public and private bodies; entertainment like games and competitions; TV voting; and legacy dial-up Internet. The provision of non-digital goods and services is increasing, for example car parking or concert tickets.

As shown in Figure 1, there is a complex value chain [(7)], with different service providers (SPs) involved, which may not all be within the same country:

- The End-user contracts with the originating electronic communications service provider (Originating CP) to access the revenue share service;
- The Originating CP bills the end-user for access to the revenue share service, and passes:
    - An agreed share of the revenue to the Service Provider/Content Provider (the called party), which may be directly allocated a number in some cases;
    - A termination charge to the terminating electronic communications service provider (Terminating CP).
- There may be Transit Providers between the Originating and Terminating CPs, which also receive payments (although in the simplest case, the originating, transit and terminating providers are on the same network).

[(7)] It should be noted that in some MS interactions between players involved could be different from those in Figure 1 (for instance, because of tax rules). However, this does not affect the general principles of sharing the revenues through the chain.

Figure 1



Considering the possibility of fraud or misuse, this has typically arisen where a party has benefitted wrongly from the additional price, above the price of using a standard geographic or mobile number.

The Handbook of the IARN [8] states that: "*As the diversity and scale of the Phone-paid sector has increased, so has the potential for consumer harm. Consumer harm* [has] *arisen involving mass-market misleading promotions for competitions and award schemes, Internet dialers with premium payment for access to web content, and mobile subscription services. The search for new revenue streams is constant and it is IARN's experience that, whilst the majority of the sector aims for compliance, not everyone will act with an appropriate level of diligence or honesty*". IARN highlighted that PRS technology facilitates access to millions of consumers on a cross-border basis from a single location with few resources, giving the ability to cause consumer harm quickly and widely.

In 2006, in its Recommendation on "*Consumer Protection Against Abuse of High Tariff Services*", the ECC within the CEPT noted that cases had arisen where end-users were

[8] See Section 2.5 for further discussion of IARN.

misled about the nature and cost of PRS (lack of transparency); suffered from unnecessarily lengthy call durations (unfair commercial practices); or numbers were used not in accordance with the relevant numbering plans. It found that “malevolent parties” might seek to become service/content providers, benefitting from existing interconnect agreements between electronic communication service providers; the end-user only has a direct contractual relationship with the originating electronic communications service provider making redress more complex; and revenues to content providers are often guaranteed by the originating electronic communications provider and paid to them before payment is received from the calling subscriber, creating financial risks at the top of the chain.

Following on from the last point, it seems that revenue share tariff numbers and services have the potential to be linked to cross-border fraud and misuse because of the global interconnection agreements between public switched telephone network (PSTN) operators. Under this arrangement, the same fees apply to all fixed calls to a country, without taking into account the higher charge for revenue share numbers or services. An actor engaging in fraud or misuse may make international calls to a revenue share number. The content provider associated with the revenue share number expects to receive a fee from the originating electronic communications provider, but the communications provider cannot recover this fee from the caller. Either the content provider, or more often the originating electronic communications provider, loses financially. The French NRA, ARCEP, noted that actors engaged in fraud or misuse could take advantage of this situation to trombone calls to their competitors, via a foreign country. Consequently, German electronic communications providers do not originate calls to foreign premium rate numbers, and Belgian and Finnish providers usually choose not to. As noted above, transposition of Article 28(1) USD in the EU might lead to changes in this respect, although the current condition of economic and technical feasibility remains. Germany and Belgium said they would expect any increase in cross-border provision to lead to an increase in cases of cross-border fraud or misuse of premium rate numbers and services.

Additionally, in its Handbook, IARN suggests VoIP is likely to facilitate and increase the cross-border provision of PRS as it means service providers do not have to seek an agreement with a network in each country.

In response to the BEREC questionnaire, NRAs identified the following examples of fraud or misuse that have occurred to date:

- End-users received an unsolicited SMS (possibly reverse-charge), letter or e-mail asking them to respond to a premium rate number or click on a WAP link, misleading the end-user about the charges and/or the nature of the service's content. In some cases, the content provider was based abroad, and made use of the numbering resources of the end-user's home country. Variants on this scenario were reported by Belgium, Germany, Malta, Poland and the UK.

NRAs reported further cases where revenue share and other higher tariff numbers and services, including satellite and SMS short codes, were linked to fraud or misuse, namely in the case of missed calls and mobile malware:

- **Missed calls**: A short 'missed call' from an international premium rate or other revenue share number was made to the end-user with Calling Line Identification Presentation (CLIP), and terminated before the end-user could answer. When the end-user called the number back, he or she incurred unexpectedly high charges. This was reported by 10 of the respondent NRAS, and is expected to continue to be a problem [(9)].

  The Calling Line Identification (CLI) can be understood as a set of parameters within telecommunications networks that provide users with capabilities of sending, receiving and displaying telephone numbers. These parameters are used in services like the CLIP, which provides the called party with the possibility to identify the subscription of the calling party via the telephone number. Their technical usage is standardized, for example, by ETSI [(10)]. Furthermore, this issue is dealt with the

[(9)] NRAs from Belgium, Denmark, France, Hungary, Malta, Netherlands, Norway, Sweden, Switzerland and UK.

[(10)] ETSI EN 300 089 (v3.1.1 2000-12); ETSI EN 300 092-1 (v2.1.1 2001-02); ETSI EN 300 356-3 (v4.2.1 2001-07).

ECTRA/ECC Recommendations [(11)], ETP Guidelines [(12)] and national regulations. Nevertheless, one might wonder if these rules require an increased level of enforcement, in order to address cases as those described by the NRAs, reported as increasing in some MS;

- **Mobile malware**: This often takes the form of a Trojan [(13)] hidden in applications downloaded over the mobile Internet. Once the phone is infected, the malware generates calls, SMS and MMS to foreign premium rate numbers, without the end-user's knowledge. This was reported by Finland.

2.1.2 Misuse of numbering plans

Just over a quarter of respondent NRAs identified instances where the numbers in the national numbering plan are subject to fraud or misuse by domestic or international providers. In some cases such misuse was a technical contravention of that MS's numbering plan without causing significant consumer harm, and in others it did cause harm to end-users. The same numbering plan rules do not apply in each MS, so that misuse in one MS may be acceptable conduct in another.

The examples most commonly given by NRAs relate to:

- **Internet diallers**: The end-user's dialler programme was hacked, to permanently change the dial-up settings from a domestic number to an international premium rate or international satellite number, without the end-user's knowledge. This was identified by around one quarter of respondent NRAs [(14)]. Cases of this type of fraud

[(11)] CEPT/ECTRA Recommendation of 22 June 2000 (ECTRA/REC(00)03) on the implementation and use of CLI (Calling Line Identification) within CEPT countries and ECC Recommendation (03)01 of 25 March 2003 (ECC/REC(03)01) on the implementation and use of CLI (Calling Line Identification) within CEPT countries.
[(12)] ETP – European Telecommunications Platform / CLI Working Group: ETP Guidelines for Calling Line Identification, Issue 4, September 2002.
[(13)] A Trojan is malware that appears to perform a desirable function for the user prior to run or install, but instead facilitates unauthorized access of the user's computer system.
[(14)] NRAs from Belgium, Greece, Malta, the Netherlands and UK.

or misuse are expected to decrease, as dial-up Internet use decreases in favour of broadband;

- **VoIP**: Four NRAs [15] gave examples where VoIP was associated with misuse or fraud linked to incorrect use of the numbering plan, for example using domestic and international mobile numbers without the consent of the provider the number had been allocated to (Finland) or presenting international numbers as national numbers (Romania). Three NRAs said they expected that incidents of fraud or misuse involving VoIP numbers and services will increase, as VoIP use becomes more common overall;

- **PABX hacking**: In a variant of VoIP being associated with numbering misuse or fraud, four [16] NRAs reported that private automatic branch exchange (PABX) software had been modified by hackers. Incoming VoIP voice traffic was then transited over the attacked PABX to foreign fixed, mobile and satellite premium rate numbers. In the Czech Republic, 7 cases were resolved, which had caused overall financial damage exceeding 180,000 Euro. The calls had been terminated in Europe (inside and outside of the EU), Africa, Oceania, and the Americas. The last Danish case of PABX hacking that the NRA (NITA) has been made aware of resulted in the victim incurring costs of roughly DKK 200.000, the equivalent of approximately 27,000 Euro. In another case reported by Romania, a company in the Netherlands complained that its *Asterisk* PBX had been hacked by an IP address that appeared to be from Romania. Several international numbers were called, with a total cost of 1,500 Euro;

- **Virtual calling cards**: Two regulators [17] reported that these have been provided by domestic and foreign operators on geographic numbers, instead of the correct access code for the service under their national numbering plan;

[15] NRAs from Finland, Latvia, Malta and Romania.
[16] NRAs from Czech Republic, Denmark, Malta and Romania
[17] NRAs from Czech Republic and Malta.

- **Audiotext:** Two regulators [18] referred to Audiotext. The Portuguese NRA, ANACOM, reported that the misuse of international numbering resources by operators inside a country occurred when numbers from a different country, not allocated by the respective NRA, were used, normally for audiotext services. ANACOM considered this situation constituted fraud, although it may not harm end-users.

The above EEC recommendation 05/09 and the ITU-T Recommendation E.156 "*Guidelines for ITU Action on Reported Misuse of E.164 Number Resources*" contain recommendations on dealing with instances of misuse or unauthorised use of international numbers, which are covered in Section 2.5 below.

2.2. Current evidence collection methods

If MS authorities may share commonalities in terms of the powers they have and the scope of the laws they enforce, certain variations remain. Some authorities are charged with resolving individual complaints, others with supervising regulatory compliance, and many do both.

Assuming that those variations may reflect on the kind of evidence MS authorities receive of cross-border problems, NRAs were invited to indicate how evidence of cross-border consumer harm related to fraud or misuse of numbering resources is currently being collected in their MS and, if possible, to indicate the level of impact of such evidence.

A few examples of evidence collection were initially included in the questionnaire, such as complaints from end-users, complaints from service providers, information collected from other bodies, but NRAs were also given the possibility of indicating any other evidence found to be relevant.

[18] NRAs from Portugal and Malta.

According to the information collected, evidence of cross-border consumer harm related to fraud or misuse of numbering resources seems to be collected mostly [19] by complaints received from end-users (from end-users themselves or through consumer associations).

Some NRAs also reported the collection of evidence from media sources or other bodies, like the Belgian NRA, BIPT, that collects evidence from the Ombudsman for Telecommunications, or the Finnish NRA, FICORA, that also collects evidence from the Data Protection Ombudsman.

Besides that, ten NRAs [20] collect evidence from providers. A few NRAs [21] also mention the police as a source for the collection of evidence.

Other NRAs do seem to have more sophisticated ways of collecting evidence. For example, the Czech NRA, CTU, which collects evidence by testing telephone numbers and monthly monitoring and reporting.

However, it is not clear if complaints received, although related to services delivered on a cross-border basis, clearly allow the recipient body to identify specific situations requiring investigation or enforcement actions – information may not be reliable or detailed enough, which makes it difficult for NRAs or other relevant national authorities to investigate it. Also, many cases of fraud or misuse of numbering resources encountered to date are, in fact, of national scope, although this might change as noted earlier in this report.

Moreover, there may be differences in the way that national authorities collect and investigate evidence – there are no reports of NRAs or other national authorities establishing common procedures.

[19] According NRAs from Belgium, Czech Republic, Denmark, Finland, Germany, Greece, Hungary, Ireland, Italy, Malta, Netherlands, Poland, Portugal, Romania and UK.
[20] NRAS from Czech Republic, Denmark, Finland, Germany, Ireland, Latvia, Malta, Netherlands, Portugal and Romania.
[21] NRAS from Netherlands and UK.

2.3. Competent national bodies for cross-border issues

As to the competent bodies currently addressing in MS cross-border problems caused by fraud or misuse of numbering resources and dealing with PRS, the most common situation seems to be where:

- The NRAs deal with electronic communications issues (numbering resources management and technical aspects of PRS);
- Other bodies may deal with other aspects of PRS, covering the content or service providers, including dedicated PRS regulators in some countries;
- The police deal with criminal issues such as fraud and misuse with criminal relevance; and
- The consumer protection national authorities handle complaints from consumers, although these are, or may be, also received by some NRAs [22].

It should be noted that communications providers themselves often play a role, for example by assessing the risk of fraud and blocking international access to numbers and services where they consider the risk is significant (providing such access is not "economically feasible" in accordance with the USD). Arguably, regulation should take into account and not seek to duplicate such activities.

2.3.1 NRAs as competent bodies

The majority of the responding NRAs [23] declare that, under the relevant national legal framework, they currently hold regulatory powers on numbering resources management and relevant PRS number management powers.

The stated PRS competencies result in general numbering resources management competencies and do not include in most cases PRS content, advertising and consumer issues related to these.

[22] NRAs from Belgium, Denmark, France, Greece, Hungary, Italy, Malta, Portugal, Romania and UK.
[23] All responding NRAs except NRAs from Hungary, Norway, Sweden and Switzerland.

Examples: France and Portugal

*The **French NRA**, ARCEP, does not have the competency to deal with PRS content issues, but remains empowered to supervise the compliance of electronic communications sector legislation and manage numbering resources according to the national numbering plan and other rules governing the use of numbers, namely, tariff caps. ARCEP also issues authorizations to providers and monitors services associated with PRS.*

*In 2009, the **Portuguese NRA**, ANACOM, was given the responsibility of verifying providers' compliance with the rules established for provision of message-based value added services under recent legislation. Before this, ANACOM had no competence on this issue. Still, ANACOM has no powers to enforce compliance with the rules on advertising of message-based value added services, which is given to another Portuguese public entity (the Consumers' General-Directorate).*

Within the previous examples, if the case is a PRS content-related one, it is often either non-regulated, self-regulated at industry-level [(24)] or regulated by another body, as it happens in the UK, where competencies over PRS are shared between the NRA and a PRS regulator, under a framework agreement, as follows.

Example: UK

The UK NRA, OFCOM, has overall responsibility for regulating PRS. However, in accordance with a framework agreement entered into with Ofcom, PhonePayPlus carries out the day-to-day regulation of the PRS market through enforcement of its Code of Practice, which requires Ofcom's approval.

Under the Code of Practice, PhonePayPlus has a range of sanctions that it may apply for breaches of the Code, including requiring suspension of access to some numbers and imposing a financial penalty.

[(24)] As it happens in Czech Republic, Finland and in France.

A specific subset of PRS ('Controlled PRS') is also subject to Ofcom's backstop enforcement powers. In relation to these PRS, compliance with the Code of Practice is mandatory. As to the other PRS, compliance with the Code of Practice is voluntary and PhonepayPlus relies on the Code of Practice being enforced by contractual chains running from the terminating operators through the PRS value chain.

Where non-compliance with a direction given by PhonePayPlus in accordance with the Code of Practice (for the purposes of enforcing its provisions) concerns a Controlled PRS, Ofcom may take enforcement action. Ofcom's backstop enforcement powers include suspending the provision of the service and imposing a financial penalty of up to £250,000.

2.3.2 Other competent bodies

From the respondent NRAs, only Sweden reported that, at national level, authorities other than the NRA are the only ones dealing with particular cross-border issues such as PRS.

Example: Sweden

The Swedish NRA, PTS, reports that the Swedish Consumer Protection Agency has regulatory powers - together with the Swedish Consumer Ombudsman - on PRS, while there are no frauds-related competent bodies, except the self-regulatory tool of an industry-led council.

2.4. Cross-border cases handled by Member States

Concerning the handling of cross-border problems already occurred in MS [(25)], it appears that a certain level of cooperation already exists between some MS to address these

[(25)] Belgium, France, Finland, Germany, Greece, Hungary, Ireland, Malta, Netherlands, Romania, Switzerland and UK.

problems and that they are most of time disposed to help each other in cross-border issues even if it is not a legal obligation.

Example: Cooperation between BNetzA and ARCEP

French non-geographic numbers are not reachable from abroad.

The German NRA, BNetzA, explains that the French NRA, ARCEP, requested for these numbers to be made available from Germany. BNetzA had no enforcement powers to impose this to network operators, but they cooperated following BNetzA's request. It is much easier for NRA's to take the necessary action if formally empowered to do so, but it is interesting to notice that informal cooperation is an existing tool.

Notwithstanding, NRAs in general consider that the transposition of Article 28(2) of the revised USD into national legislation could be an opportunity to strengthen cooperation.

A number of NRAs deal at a national level with numbering misuse by blocking specific numbers. Five respondent NRAs [(26)] mentioned the blocking of numbers as a way to resolve misuse of numbers at an international level. Some MS have adopted legislation and decisions that organize the blocking of numbers in certain situations; others have blocked specific numbers in order to deal with a particular case.

Examples: Greece and UK

*The **Greek NRA**, EETT, reported a particular situation related to internet dialler fraud, causing calls to unusual destinations. After examining customers' complaints, EETT collected traffic data by the operators and issued a decision to oblige the operators of public fixed telephony services to temporarily bar the direct calls made to a specific list of international destinations and routing all subscribers' calls through a live operator service. All ISPs had to inform their subscribers of the threat and suggest means of protection.*

[(26)] NRAs from Belgium, Finland, Greece, Malta and UK.

Operators were compelled to send periodically (every 15 days) to EETT traffic data as to specific international numbers. The restrictions were removed some months later.

*The **UK NRA**, OFCOM, underlines that it has some means at its disposal to deal with misuse (blocking of numbers, fines etc.) and that any communications provider wishing to continue to operate in the UK market must comply. In particular, it cannot have dealings with other providers in the value chain that infringe the UK PRS rules, even where they are based outside of the UK.*

However, other NRAs underline that they do not currently have the power to require, at least not under all circumstances, the blocking of numbers or withholding of interconnection or other service revenues. In some cases, certain countries have to appeal to cooperation with network operators so that they voluntarily block the numbers; the NRA is not able to impose it. Belgium reported the recent adoption of legislation in order to entitle the NRA to block numbers. Finland reported that the NRA is able to impose blocking/withdrawal of numbers in case of misuse of numbering resources or measures to implement information security. In cases where fraud is related to the content of the service (which does not breach information security), the NRA does not have powers to block the numbers.

Respondent NRAs also very often refer to information as a way to deal with cross-border issues. When confronted with them, some NRAs indicated that they provided information on their websites, or on other relevant Internet sites, in order to warn consumers.

2.5 Existing international cooperation mechanisms

According to the 2006 OECD **Report on Cross-Border Enforcement of Privacy Laws**, "*enforcement co-operation "seems instinctively to be a 'good thing'. As information and communications networks have grown in size and capabilities, the business and operational efficiencies they bring have been accompanied by increased privacy risks. Mitigating these risks while at the same time ensuring the trust needed in a global economy dependent on the free flow of information requires strong cross-border privacy law enforcement co-operation*."

Having that in mind, in response to the BEREC questionnaire, NRAs were invited to identify international cooperation mechanisms, both those that they considered likely to be relevant to the scope of Article 28(2) of the revised USD and those that, although likely to fall outside that provision's scope, could provide useful experiences for BEREC to learn from or build upon when considering any cross-border aspects of transposing Article 28(2).

So far, the information collected allows BEREC to identify several different mechanisms, most of them relevant to the scope of Article 28(2), but also some outside its scope. Below is a brief description of the options identified by respondent NRAs [(27)].

a) Relevant mechanisms within the scope of Article 28(2) of the revised USD:

- **International Audiotex Regulators Network** (IARN): Established in 1995, IARN defines its main objectives as encouraging information exchange and raising awareness of the regulation of the audiotex industry and the regulatory approaches of its member countries. IARN also aims to ensure that the development of phone-paid services within the EU (and beyond) goes hand-in-hand with effective consumer protection.

  In particular, IARN acts as a forum for the exchange of good practices and information about the regulatory methods and legal and administrative arrangements in different countries (Government regulation, co-regulation, and self-regulation, including enforcement mechanisms); maintains a set of non-binding principles of regulation, which represent a minimum standard of consumer protection and may be exceeded by some members (in the 'IARN handbook'); facilitates contacts between regulators to enable working-level co-operation to identify and deal with malpractices; remains accessible to all relevant regulators (not only current members); promotes awareness of the Group in the international arena; and exchanges information with international regulatory organisations (in particular the EC).

[(27)] As identified by Belgium, Czech Republic, Finland, Germany, Italy, Norway, Portugal and Romania.

IARN has 23 members including from 15 EU MS: in Denmark, Germany and Poland this is an NRA member of BEREC, and in Austria, Belgium, Cyprus, Czech Republic, Finland, France, Ireland, Netherlands, Romania, Spain, Sweden and the UK this is another national body. It actively encourages contact and the development of closer ties with other countries where phone-paid services are consumed.

IARN has a rotating Chair, ad hoc working groups to deal with specific topics, and biannual Plenary meetings. Plenary meetings aim to: enable the exchange of information and the discussion of shared concerns; develop a set of agreed regulatory principles and enforcement practices that provide consistent cross-border protection to consumers.

Discussions are currently underway between its members on how to further develop and deepen IARN's cooperation activities, in light of developments in the types of PRS (e.g. use of mobile handsets as tickets, money transfer, location-based services) and related technologies (handsets, digital TV, faster mobile networks, VoIP growth facilitating cross-border provision).

Although at this time IARN does not have members from all EU countries and does not have the funding that would be required to play a formal coordination role in relation to cross-border enforcement for PRS, its aims and approach provide interesting examples of possible cooperation mechanisms in this space.

- **Consumer Protection Cooperation** (CPC): Regulation (EC) No. 2006/2004 on Consumer Protection Cooperation was adopted to tackle the growing cross-border problems where traders exploited the Internal Market to target consumers in other EU MS with dishonest practices. It lays down the framework and general conditions under which authorities, responsible for enforcement in the MS, are to cooperate to ensure compliance with consumer laws, the smooth functioning of the Internal Market, and the protection of consumers' economic interests. It covers consumer law in a variety of areas inside and outside of BEREC's areas of competency, including misleading advertising and distance selling. It formally started operations in 2006-7.

The Regulation sets up an EU-wide network of national enforcement authorities with similar investigation and enforcement powers, through which the authorities must, on request, assist other members by investigating possible breaches of consumer laws originating in their territory and having effects in the requesting MS. They must also assist by taking enforcement action, and notify other MS and the EC of any investigations being pursued as a result of a request. If certain conditions are met, MS may refer enforcement to another national body.

Additionally, the authorities are required to coordinate their market surveillance and enforcement activities, and exchange all necessary information to this end. When they become aware that an infringement within the EU harms consumers in more than one MS, the authorities shall seek to carry out simultaneous investigation and enforcement activities.

The Regulation sets out the procedures for requesting mutual assistance: it must contain sufficient information to enable a requested authority to meet the request including any evidence only available in the territory of the requesting authority. Requests must be sent from and to the identified, single liaison offices of the relevant authorities, using a standard form, using a special database also established by the Regulation. The Regulation also contains provisions on data protection and privacy, information exchange with third countries (subject to bilateral agreement between the requesting and requestor authorities), costs incurred by requested authorities (not recoverable, except for costs and losses incurred as a result of measures held to be unfounded by a court regarding the substance of the intra-Community infringement), and the conditions for refusing a request (judicial proceedings have been initiated; investigations reveal no infringement; the requesting authority did not provide sufficient evidence with its request).

MS also use the network to share expertise with other authorities and the EC, on training, complaints handling, development of sector-specific networks and information tools, guidelines and exchange of officials.

- **International Consumer Protection and Enforcement Network** (ICPEN): this is an international network of governmental consumer protection authorities from 38

countries including 23 EU MS. Its long-term aims are to generate and share information and intelligence about cross-border commercial activities that may affect consumer interests, share best practices in legislative and enforcement approaches to consumer protection, take action to combat cross-border breaches of consumer laws, facilitate effective cross-border remedies and encourage international law enforcement cooperation.

The network has devised econsumer.gov (established in 2001, 24 member countries, including 14 EU MS), a multilingual website where consumers may lodge cross-border complaints, which are accessible to certified government agencies in ICPEN member countries. They may use this information to investigate suspect companies and individuals, discover new scams, and identify trends in fraud. The website also provides advice to consumers on resolving their disputes through alternative resolution mechanisms.

ICPEN has a rotating Presidency and holds biannual plenary conferences to exchange experiences on prevention and enforcement. Much of the network's activities take place in working groups. It also runs regulator joint activities, including monitoring and best practice training.

- **ITU Recommendations on numbering resources**: Numbering resources are allocated, structured and their use defined by a series of ITU-T Recommendations. Among those recommendations, there is **ITU-T 2006 Recommendation E.156, Guidelines for ITU-T action on reported misuse of E.164 numbering resources** – different groups of E.164 international numbering resources have different assignment criteria, and therefore different forms of misuse may be identified.

  Where the misuse is alleged to occur in relation to the use of an international numbering resource, then the procedures in Recommendation E.156 shall apply. Those procedures include MS using a standardised notification form to inform the Director of the Telecommunication Standardization Bureau (TSB) of situations that indicate possible misuse of numbering resources. Depending on the numbering resource, the TSB Director informs the relevant parties, invites representations, and disseminates information;

- **ECC Recommendation on "Customer Protection in Case of Misuse or Unauthorised Use of International E.164 Numbering Resources"** (ECC/REC/(05)09): This recommendation, dated 2006, proposed complementary measures to the ITU-T procedures for reporting potential misuse of international numbering resources, including the 'Early Alert System' (EAS).

  The EAS is a channel for information exchange between NRAs that have decided to participate the system. All actions, if any, and responsibilities are taken on a national level. The information exchanged within the EAS is restricted to the participating NRAs. It is a national matter how to exchange information between the NRA and market parties.

b) Relevant mechanisms outside the scope of Article 28(2) USD:

- **European Government CERTS (EGC) group**: this is an informal group of governmental computer security incident response teams (CSIRTs) that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe. Its members are Finland, France, Germany, Hungary, Netherlands, Norway, Spain, Sweden, Switzerland and the UK.

  To achieve this goal, the EGC group members jointly develop measures to deal with large-scale or regional network security incidents; facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities, identify areas of specialist knowledge and expertise that could be shared within the group, identify areas of collaborative research and development on subjects of mutual interest, encourage formation of government CSIRTs in European countries, communicate common views with other initiatives and organizations;

- **Rapid Alert System for all Dangerous Consumer Products (RAPEX)**: This EU system allows for the rapid exchange of information between MS via central contact points and the EC of measures taken to prevent or restrict the marketing or use of products posing a serious risk to the health and safety of consumers (white paper

warnings are also issued). It also includes a data base of companies previously involved in fraud, telephone numbers subject to misuse or fraud, particular practices identified;

- **European Advertising Standards Alliance (EASA):** EASA promotes responsible advertising by providing detailed guidance on how to go about advertising self-regulation across the Single Market for the benefit of consumers and businesses. This includes information and expertise sharing, as well as the Cross-Border Complaints (CBC) system between European advertising self-regulatory organisations.

  The Cross-Border Complaints (CBC) system is an agreement by which all members of EASA agreed to handle cross-border complaints under the same conditions as national complaints. Under the CBC, there is a definition of the complaints considered cross-border and which, for that reason, fall within the scope of the CBC. Also, there are two basic principles to CBC. The first is 'country of origin', according to which an advertisement must comply with the rules of the country where the media is based (or in the case of direct mail advertising, the country where the advertiser is based). The second principle is 'mutual recognition', meaning that EASA members agree to accept advertisements, which comply with the self-regulatory rules in the country of origin of the media, even if those rules are not identical to their own.

3. Practical implementation of Article 28(2) USD

This section aims to provide a high-level description of how NRAs anticipate that paragraph 2 of Article 28 of the revised USD may operate in practice, specifically what measures or procedures they consider important to put in place to allow NRAs (or other relevant authorities) to effectively use that provision, based on the responses from 22 NRAs to the questionnaire on cross-border issues circulated between May and June 2010.

However, BEREC notes that:

- Most of the MS have not yet concluded the transposition of the revised regulatory framework and some of them are still at an early stage of that process. Therefore, they cannot anticipate, yet, the terms according to which the mechanisms foreseen in Article 28(2) of the USD will be implemented;

- Some NRAs do not have or will not have specific competencies in this field; also, the project of transposing the Directive is in some cases a responsibility of the competent national ministry, of which the NRA is not aware;

- While some services clearly lend themselves to a pan-European approach e.g. international roaming, in most markets most services within the scope of the regulatory framework are not traded across national borders. Therefore, cross-border issues are not among NRAs or other relevant authorities' greatest concerns.

In addition to the "formal" responses of each NRA, it was also possible to capture from few of the respondents their expert views on the practical implementation of Article 28(2) of the USD, to be considered for informative purposes only and not to be attributed to the corresponding NRA.

3.1. Who are expected to be the relevant national authorities?

The questionnaire circulated to the NRAs also aimed to gather information on the institutional bodies that – within the scope of the national transposition legislative processes

– are expected to be entrusted with the new competencies in the event of cross-border fraud or misuse of numbering resources.

Such issues arise with reference to the specific wording of Article 28(2), which refers to the "relevant authorities" as the authorities that are to be entrusted with the new above-mentioned competencies.

Based on the 22 contributions received, responding NRAs could be divided into three groups:

a) The large majority of NRAs expect that the "relevant authorities" as in Article 28(2) of the USD to be formally designated by means of the national transposition provisions, are the electronic communications regulators, although another national authority may be designated in addition;

b) Only three of the responding NRAs (CTU, PTS and FICORA) believe instead that the new tasks will be fully assigned to other bodies;

c) All the others do not provide a clear view on the matter, mostly referring to the ongoing national transposition proceedings.

By and large, it can be observed that contributions provided by responding NRAs on the subjects (the "relevant authorities") that they expect to be charged to implement the new competencies, could be considered as related to the nature and the extension of the institutional tasks already entrusted to electronic communications regulators under the relevant national legal frameworks as regards numbering resources management and PRS.

As a matter of fact, in general terms, the projection elaborated by the majority of the responding NRAs – of being entrusted with the new competencies – seems to be reasonably related to the fact that they declare to currently hold regulatory powers on numbering resources management and PRS.

NRAs stating that they expect not to be charged to carry out the new tasks, also inform that they have separate national regulators for PRS in particular, for consumer protection

including relating to fraud or misuse of numbering resources, and/or that the issue is dealt with by industry self-regulatory tools (for example, the last two exist in Sweden).

In the group of NRAs not providing clear indications on the bodies that they expect to be entrusted with the new powers, the electronic communications regulator does not hold at present exclusive competencies on PRS market, as explained more in detail in the paragraphs ahead with respect to the 3 NRAs concerned.

It is not possible to identify the same correlation between NRAs answers to the questionnaire, when invited to report if they are expected to be a "relevant authority" mentioned in Article 28(2) USD, and NRAs' regulatory competencies in cases of frauds or misuse of number ranges, as in answers received about any other bodies involved in regulating fraud or misuse of number ranges that may result in consumer harm. On this latter, competencies are indeed spread amongst several bodies, including police authorities.

In the following paragraphs, a more detailed analysis is provided of the features of the 3 above-mentioned groups in which the 22 responding NRAs can be divided.

a) Responding NRAs expecting to be entrusted with the new competencies

Twelve out of the fifteen NRAs envisaging to be entrusted with the new tasks, already have exclusive competencies on numbering resources management based on their relevant numbering plans and therefore already carry out PRS regulation (essentially not on the content provided).

Examples: NRAs expecting to be entrusted with the new competencies

Based on the fact that it already has responsibilities in the field of numbering resources management and interconnection relations supervision, the ***Belgium NRA****, BIPT, envisages to be entrusted with the new powers upon adoption of the transposition law; however it does not hold at present exclusive competencies on PRS regulation, as this is delegated to the Ethical Commission for Telecommunications, which is only supported by BIPT by means of a Secretariat.*

*The **Italian NRA**, AGCOM, is also in this group of NRAs; however, it currently shares competencies on numbering resources management and PRS with the Ministry for Economic Development: AGCOM's remit on this issue covers the numbering plan definition and the relevant consumer protection, whereas the Ministry shall adopt PRS-related regulation and carries out the supervisory activities regarding the conformity of numbers usage (also PRS numbers) with the numbering plan, also upon AGCOM recommendation.*

*The **Dutch NRA**, OPTA, shares competencies on PRS with the Consumer National Authority.*

Overall, from the information collected, it seems possible to affirm that NRAs expecting to receive the new competencies are generally entitled with powers pertaining to numbering resources management and also PRS numbers, but not to the relevant content provided nor to the question of fraud.

b) Responding NRAs expecting not to be entrusted with the new competencies

Three of the respondent NRAs believe that they will not be entrusted with the new competencies as in Article 28(2) of the USD.

Examples: NRAs expecting not to be entrusted with the new competencies

*The **Czech Republic NRA**, CTU, points out that the national transposition is ongoing and that - despite holding competencies over PRS numbers - it expects that the new tasks will be assigned to the police or other authorities with investigation powers in face of frauds (such as a Ministry). In terms of competencies already held by CTU and their possible impact over this NRA's projection, it should be highlighted that today, in the Czech Republic, competence over SMS/MMS short codes is not in CTU's hands, but it is basically coped with by industry's self-regulation. Also in terms of fraud, CTU does not hold any competence. However, it does have numbering resources management powers.*

*The **Swedish NRA**, PTS, expects not to be the designated "relevant authority" and indicates the Consumer Protection Agency as the proposed authority; this authority has indeed*

regulatory powers - together with the Consumer Ombudsman - on PRS, while there are no fraud-related competent bodies, except the self-regulatory tool of an industry-led council.

*The **Finnish NRA**, FICORA, expects the Consumer Agency to be entrusted with powers relevant to new Article 28(2) implementation; such authority could be empowered indeed to block access to PRS in case of fraud or misuse related to the content of the service. FICORA's powers concerning fraud issues will be based on current provisions in the Communications Act and in the Act on the Protection of Privacy in Electronic Communications. FICORA currently holds powers in numbering resources - therefore also PRS numbers – management.*

c) Responding NRAs where more than one national authority currently has a relevant role

Other three of the respondent NRAs do not yet have a clear overview of which authority will be entrusted with the new competencies, given that transposition proceedings are ongoing and more than one national body currently has a role in the relevant areas.

Examples: Overview of answers received

*The **UK NRA**, Ofcom, refers to the currently ongoing evaluation of the new Article 28(2) of the USD implementation. In terms of the NRA's current powers on PRS in the UK Ofcom retains the overall competence on PRS; however, it has signed an agreement with PhonePay Plus which is today the PRS Regulator in the UK, enforcing its Code of Practice (adopted upon Ofcom's approval) in the PRS market. Previously known as ICSTIS, this body regulates phone-paid services in the UK, as the premium rate goods and services, which people can buy by charging the cost to their phone bill and pre-pay account.*

*The **Hungarian NRA**, NMHH, identifies other authorities that may be involved upon conclusion of the national transposition process: the National Competition Authority and the National Consumer Protection Authority, which have indeed powers in case of fraud or misuse.*

*The **Norwegian NRA**, NPT, reports of a decision-making process ongoing as regards the assignment of the relevant competencies; at present, the NRA has competence only over the sector framework regulation, whereas consumer authorities provide the specific regulation as well as the industry standards.*

3.2 How is Article 28(2) USD expected to operate in practice regarding the blocking of numbers/services and withholding of interconnection revenues?

3.2.1 Cases where the "relevant authorities" include the NRA

Prior to the adoption of the Framework Review package in November 2009, the previous work done by ERG, identified the proposal for Article 28 of the USD as intending, among other aspects, to address the case of a consumer in country A being victim of fraud/misuse when calling a number in country B.

Practical issues to be solved

The relevant authorities will need to consider how, in practice, they can take the enforcement actions contemplated in Article 28(2) USD – requiring undertakings to block access to numbers and/or services and to withhold interconnection or other service revenues.

This means that each MS is left with the task of defining such aspects at a national level, including consideration of some of the key issues identified by the previous work done by ERG.

Having in consideration the questions raised by Article 28(2) of the USD, as well as the practical difficulties illustrated by the example above, BEREC has gathered views from NRAs across Europe on how this provision is expected to operate in practice, to enable the NRA (where it is a "relevant authority") to require networks and/or providers to block access to numbers/services and withhold related interconnection and other service revenues.

Key findings

Half of the 22 responding NRAs presented a specific view on how they expect Article 28(2) USD to operate in practice, to enable the "relevant authorities" to intervene.

The other half was in general reluctant to do so, given the reasons highlighted earlier, mostly the early stage of the national transposition process of the revised regulatory framework. Nonetheless, some of the responding NRAs already expect the transposition process to bring some changes to the NRA's current enforcement powers. As an example, the Dutch NRA, OPTA, which currently only has powers to require blocking of certain PRS numbers in case of misuse, said it might be empowered to require undertakings to block access to other numbers as well and to take action in the case of fraud, following the transposition of the revised regulatory framework.

Focusing on the NRAs that gave a specific view, some cases are worth looking at in more detail, as they point out some interesting ideas, and even some common concerns, about the terms in which NRAs would exercise their powers to require the blocking of access to numbers and withholding of interconnection or other service revenues under Article 28(2) of the USD, if they are a relevant authority.

Example: Germany

The German NRA, BNetzA, was the only NRA reporting that Article 28 USD was already implemented, by § 67 of the German Telecommunications Act. For BNetzA enforcement actions according to that provision are only possible concerning unlawful behavior in Germany.

Within that scope, the NRA, under its responsibility for numbering administration, may issue orders and take any other suitable measures to secure compliance with legal provisions and with the conditions it has imposed in connection with the assignment of numbers. The NRA may also require undertakings to provide information on personal data, such as the name and address for summons of number holders and number users, provided the data are known to the undertakings – in particular, the NRA may request information on personal data required for an examination of obligations in individual cases when it has received a

complaint or when it assumes a violation of duties for other reasons or carries out investigations on its own initiative.

Where statutory obligations or obligations imposed by public authorities have not been fulfilled, the NRA may even withdraw the unlawfully used number. Further, where it has reliable information on the unlawful use of a telephone number, it should issue an order in relation to the operator of the network in which the number is activated to deactivate it. Also, the NRA may, where it has reliable information on unlawful use, request the bill issuer not to issue bills for the number concerned. In justified exceptional cases the Federal Network Agency may prohibit certain categories of dialer.

Example: Finland

Although Article 28(2) of USD has not yet been implemented, the Finnish NRA, FICORA, reported that there is already a draft in preparation, according to which the Consumer Agency can require operators to block access to a number or service if the service is generating fees on the communication service invoices by fraudulent action. The Consumer Agency may also require operators to withhold the revenues for the service and pay them back to end-users deceived.

Those provisions will be added to obligations or powers already in force, namely Section 131 of the Finnish Communications Market Act, which provides that "If a communications network or equipment item causes danger or interference to a communications network, equipment, communications network user or another person, the telecommunications operator or the keeper of another communications network or equipment shall take measures immediately to rectify the situation and, if necessary, isolate the communications network or equipment from the public communications network". In such cases, the Finnish NRA may order rectification measures, as well as the isolation of the network or equipment. FICORA can also react to certain fraud cases based on Section 20 of the Act on the Protection of Privacy in Electronic Communications, which provides measures for implementing information security.

Example: Belgium

While transposing the revised regulatory framework, the Belgian NRA, BIPT, contemplates imposing the blocking of access to a number subject to misuse and the withholding of the relevant interconnection payments on the originating side (so in country A, country of the harmed end-user, even if a number from country B is used or even if the service is offered from country B (more frequent)).

For information purposes only, the Belgian respondents also considered as beyond discussion that withholding interconnection or other revenues needs to be done in country A, otherwise, the provision does not seem to have much use in practice.

From the examples highlighted as well as from all the information collected, there are some common points to be noted:

- A number of NRAs considered of primal importance to make the provision effective, that executive powers of authority are granted to NRAs or other relevant authorities, which allow them to act in order to implement the provision;

- Most NRAs do expect to be empowered in order to be able to require undertakings, at a national level, to block access to numbers. However, regulation of assignment of numbering resources and blocking number procedures should clearly establish on which cases NRAs may intervene and what type of powers they can call on;

- NRAs seem to consider that blocking access to numbers will be adequate to react, on a case-by-case basis, mostly against the misuse of numbering resources, understood by some NRAs as the failure to comply with legal provisions and with the conditions imposed in connection with the assignment of numbers;

- NRA ability to require undertakings to block services was not anticipated in most of the responses. This may perhaps be explained by one of two reasons: either because NRAs would have the ability to block numbers instead, which many of them considered adequate, or because another authority will have this power;

- A number of NRAs also expect to be empowered in order to be able to require undertakings, at a national level, to withhold interconnection or other service revenues, mostly to react against the misuse of numbering resources;

- NRAs anticipate this enforcement action to be implemented in different ways – in some cases, NRAs may request the bill issuer not to issue bills for the number concerned; in other cases, NRAs may require undertakings to withdraw the revenues and pay them back to end-users;

- NRAs ability to require undertakings to block access to numbers or services, as well as to withhold interconection or other service revenues by reasons of fraud was not anticipated in most of the responses: as an example, the Greek NRA (EETT), in reference to the possibility of blocking interconnection or other service revenues, assumes that it will be difficult for the NRA to impose such a measure, since determining fraud is not within its jurisdiction. BEREC notes that cases of fraud may fall within the competencies of criminal enforcement authorities;

- Whatever the terms of the transposition of the revised regulatory framework into national legislation, the large majority of respondent NRAs enphasize the primal importance of cooperation between relevant authorities in different MS for the purposes of Article 28(2) USD, making it easier to implement.

Areas where cooperation might be needed between NRAs

Given the importance of cooperation between relevant authorities for the purposes of Article 28(2) of the USD, NRAS were also invited to state on what particular aspects of enforcement they envisage cooperation between NRAs to be necessary or important.

From the responses received, it is possible to identify specific areas where cooperation might be needed between NRAs, as follows:

a) At an early stage, when there is still no proven fraud or misuse

Most of the responding NRAs seem to be in favor of adopting forms of cooperation at an early stage, when there is still no proven fraud or misuse, perhaps only anecdotal evidence of harm to end-users. In such a way, cooperation between NRAs could be important for making each of them alert, to allow them to confirm if there is justified reason for alarm and, if so, to consider action to prevent the widespread of fraud or misuse of numbering resources. Sharing information would be the basis of this kind of cooperation system. The most relevant source for NRAs to provide information would be end-user complaints, received directly by the NRAs or by other relevant/competent national authorities to be reported to the NRAs. Information to be shared could circulate by existing communication channels between NRAs or even by channels to be designated for this specific purpose (e.g., a contact list of people handling these issues in each NRA);

Example: Belgium

BIPT suggests that procedures for confirmation should be as light as possible, for instance, through direct e-mail exchanges, since consumer harm increases over time.

Also at an earlier stage, a reduced number of respondents seem to be in favor of NRAs cooperating in order to work out common practices and approaches for action in similar cases, even suggesting, in one case, that exchanging experiences at this level could be important for improving regulation in order to avoid any possible harm that misuse of numbering resources might cause to end-users.

b) As a relevant step for the purpose of investigating and executing enforcement actions whenever confronted with evidence of harm to end-users

A significant number of responding NRAs envisaged cooperation also as a relevant step for the purpose of investigating and executing enforcement actions, at a national level and within NRAs competencies, whenever confronted with evidence of harm to end-users.

According to some responses, while investigating and under cooperation procedures, a particular NRA could request information from other NRAs about a specific number, service

or provider involved in a case under investigation due to complaints received from end-users.

Cooperation would also make it possible for NRAs to proceed with enforcement actions, as follows from the examples.

Example: UK

The UK NRA, OFCOM, highlighted a specific case in which they consider co-operation between NRAs as most useful: where a scam involves a consumer ringing an international phone number. In such a scenario, the NRA where the consumer is based is unlikely to be best placed to ensure that access to the service is blocked.

Example: Finland

FICORA suggested that information could be delivered by the NRA of the MS in which numbers are being blocked, to the NRA in another country so that the other NRA could also take actions against the service provider (or ask the relevant national authority to do so). Information sharing in general concerning fraud (methods, statistics, etc.) could be useful, taking the example of GovCERT, a Computer Emergency Response Team working in several European countries by assisting public sector organizations in the response to computer security incidents and providing advice to reduce the threat exposure. Its work is also based on information sharing concerning information security threats and incidents.

Furthermore, a number of NRAs stated that after a case of fraud or misuse is identified, investigated and compliance action taken, it would be useful to promote the exchange of experiences between NRAs for improving regulation in order to avoid any future harm from the misuse of numbering services.

What harmonized or standard procedures could be implemented between NRAs?

NRAs were also invited to state what harmonized or standard procedures could be implemented between them, in order to ensure that Article 28(2) USD is put in place in an effective way.

At this stage in transposition, most NRAs were only able to say that the implementation of harmonized procedures would be very useful.

A number of MS, however, seemed to concur on the establishment of agreements between NRAs, without particular requirements of formality that could cover information-sharing, handling of cross-border complaints, standards of evidence required for penalties and enforcement.

Example: Norway

The Norwegian NRA, NPT, warned that as the national regulation of PRS varies considerably in the world and not all NRAs have full powers on this matter, it is going to be a challenge to create good harmonizing processes. However, they believe this will be possible looking at the handbook of IARN and the previous work of the former Working Group NNA of the ECC (now the Working Group on Numbering and Networks (WG NaN)), and that this could be discussed at a joint session – between NaN, IARN and BEREC.

Even in the absence of such agreements, taking into account the powers that all NRA's already have, or will receive following the transposition of the revised regulatory framework, cooperation between them and/or with other relevant authorities in order to ensure the enforcement of Article 28(2) of the USD would still be possible.

A small group of NRAs went a little bit further in their suggestions, by considering it important to have not only harmonized but standardized procedures, in order to receive complete guidance on how to act in situation of a cross-border fraud or misuse of numbering resources. Those NRAs seem to agree on an approach where BEREC plays an important role in standardization.

Examples: Italy and Lithuania

The Italian and the Lithuanian NRAs, AGCOM and RRT respectively, suggested a similar forum for standardized proceedings to be defined. AGCOM suggested this subject to be handled at the BEREC Project Team handling end-users issues.

3.2.2 Cases where other "relevant authorities" may be designated

Within the 22 responses collected *via* NRA questionnaire and as concluded earlier in this section, cases involving MS where at least one of the relevant national authorities is not the NRA are a minority.

Also, when anticipating how Article 28(2) USD will operate in practice, specifically what measures or procedures are being considered or are felt to be needed to allow relevant authorities other than the NRAs to effectively use the provision, information is limited at this stage in the transposition process, leaving several questions without answer.

Nevertheless, the situation reported by Sweden appears to be a relevant example of Article 28(2) USD operating under other practical arrangements, specifically on the measures or procedures that are being considered or are felt to be needed to allow relevant authorities other than the NRA to effectively use that provision.

Example: Sweden

In Sweden it is the Consumer Protection Ombudman (CPO), which may decide that an undertaking providing electronic communications networks or electronic communications services is to block access to a number or a service whose marketing is unfair, fraudulent or represents misuse. This decision may only be taken as consequence of CPO initiating a procedure against the holder of a number or service provider on the same grounds.

4. Proposed approach for further work

This section aims to identify areas where further work is needed, mostly within the context of the transposition into national legislation of the new version of Article 28 of the USD, and to present proposals accordingly.

The following proposals have taken into consideration all information collected from the 22 NRAs that have responded to the questionnaire on cross-border issues, the relevant inputs taken from the previously completed report on cross-border enforcement, research carried out by BEREC while producing this report and, lastly, comments received in response to the stakeholder consultation on a draft version of this report.

- Definition of “misuse” and “fraud” for the purpose of Article 28(2) of the USD;
- A contact list of the “relevant authorities” for the purposes of Article 28(2);
- A minimum set of responsibilities that should be given to “relevant authorities”;
- Provision of information by undertakings to relevant national authorities in the context of compliance actions;
- A minimum and common set of enforcement actions should be defined by MS;
- Practical cooperation mechanisms between “relevant authorities”;

4.1 Definition of “misuse” and “fraud” for the purpose of Article 28(2) of the USD

Article 28(2) of the USD requires MS to repress particular situations that are able to compromise cross-border access to numbers or services, i.e. fraud or misuse. However, the USD does not provide a definition of these situations, leaving to MS’ jurisdiction the power of establishing their own definitions. The risk inherent to this scenario is that different criteria may be settled by each MS to justify enforcement actions to be taken as in 28(2) USD, potentially hindering the aim of harmonisation and cooperation.

Most NRAs seem to consider that blocking access to numbers will be adequate to react, on a case-by-case basis, mostly against the misuse of numbering resources, understood by

some NRAs as the failure to comply with legal provisions and with the conditions imposed at a national level in connection with the assignment of numbers.

Still, a common definition to all MS of what is considered misuse and what situations may be included is required, in order to address questions such as misuse being only misuse of numbering resources or other practices too. For this purpose, particular attention should be given to international recommendations in force that already address this issue, as discussed earlier in Section 1 (1.2). In response to the public consultation, one of the stakeholders [(28)] considered useful further analysis by BEREC on how to avoid the increasing misuse by / of services in certain numbering ranges and related fraud in the EU along with studying the increased use of ITU-T international numbering in the EU.

On the other hand, NRAs ability to require undertakings to block acess to numbers or services, as well as to withhold interconnection or other sevice revenues by reasons of fraud was not anticipated in most responses. This may be explained by the fact that, in a significant number of cases, determining fraud is not within NRAs remit or they may only have limited competency to do that.

Although the transposition of Article 28(2) USD into national legislation may give new or reinforced role to NRAs – if designated "relevant authorities" (as they may, under that provision, be given the necessary ability to require blocking access to numbers or services and withholding interconnection and other service revenues by reasons of fraud, in addition to misuse), the USD does not provide a definiton of fraud for the specific purpose of Article 28(2), since this is a concept which goes beyond electronic communications services and relates to criminal law.

There are different practices that can be considered as fraud. As we have seen from the information collected from the respondent MS, most of the fraud operates with traffic creation against PRS numbers, sometimes without the awareness of the end-user, which can be done in several ways. But there are other forms of fraud and some of them are only considered as such by a few MS.

[(28)] European Telecommunications Network Operators' Association (ETNO).

The Unfair Commercial Practices Directive, Directive 2005/29/EC of the European Parliament and of the Council, of 11 May 2005, introduced common rules on, *inter alia*, misleading, deceptive or aggressive commercial practices directed to consumers.

As a general principle, the directive outlaws practices that are contrary to the requirements of professional diligence and distort or are likely to distort the economic behaviour of an average consumer in relation to a product. In particular, commercial practices must be regarded as unfair if they are misleading or aggressive.

Misleading commercial practices can be actions or omissions. Misleading actions are commercial practices that lead the average consumer to purchase (or not) a product or service because of a deceptive practice. Misleading omissions cover commercial practices that omit basic information that the average consumers needs in order to make a decision. Limitations imposed by the communication medium can however be taken into account to assess whether there is an omission.

The Unfair Commercial Practices Directive also contains a list of commercial practices that in all circumstances have to be considered unfair by the MS, without further assessment. They include:

- creating the false impression that the consumer has won or will win a prize or other benefit (when in fact the consumer must incur a cost to claim the prize);
- falsely stating that the product or service will only be available for a very short time;
- sending advertisements with a direct exhortation to children to buy, or to persuade their parents or other adults to buy, advertised products for them;
- making persistent and unwanted solicitations by telephone or e-mail or other remote media...

Practices other than those listed can also be considered as unfair on a case-by-case basis when they are in breach of the provisions of the directive.

From the above, it follows that a coordinated approach to misuse and fraud under Article 28(2) USD may be elaborated. This could be achieved by describing the catalogue of national practices that are considered as fraudulent or misusing in a cross-border context. It

can be clarified if practices to be included in that catalogue should cause proved harm to end-users. The practices in the catalogue would not be accepted and their proved occurance would be the justification for NRAs and other “relevant authorities” to require undertakings to block access to numbers or services and withhold interconnection or other service revenues.

However, this cannot lead to the identifcation of a common definition of fraud, as this may impact on the legislation of each MS, especially if it implies particular practices to be considered as a criminal offense not yet considered as such at national level; implementation problems may therefore arise due to diverging national definitions of fraud within the scope of criminal laws across the EU MS.

4.2 A clear definition of the “relevant national authority” for the purposes of article 28(2) USD

The “traditional” NRAs for electronic communications, due to their particular responsibilities in numbering and interconnection activities, are already being anticipated by most MS as the “relevant authorities” as in Article 28(2) of the USD to be formally designated by means of the national transposition provisions.

Still, there are some MS that have specific regulators for PRS services or other types of organisations or bodies, such as consumer protection bodies, that are believed to be entrusted with powers of authority in accordance with Article 28(2) of the USD.

At the same time, cases where several national authorities exist that may be possible candidates to the position of “relevant authority”, may lead MS to transpose Article 28(2) USD by establishing a shared powers of enforcement system between NRAs, consumer protection bodies, specific regulators for PRS, if they exist, and even the police for fraud issues. In such an event, there is a high-level risk of overlapping competencies between different authorities at a national level or of an unclear definition of which authority is responsible for acting in each particular situation, which could certainly be an obstacle to prompt enforcement actions to be taken.

A pre-condition for proper and safe access to services using non-geographic numbers within the Community and access to all numbers provided in the Community is that “relevant

authorities“ as in Article 28(2) of the USD are assigned in each MS and that they have clearly defined powers.

The names of these authorities should be informed to BEREC, that should have a permanently updated list of the competent bodies responsible for the enforcement of Article 28(2) of the USD.

BEREC recognises, however, that in the event that practices under Article 28(2) of the USD, namely fraudulent practices, are deemed to have criminal relevance, in some MS the enforcement of that provision by a “relevant authority” would depend on a prior decision from a national court. This requirement may be difficult to reconcile with the speed that this kind of process should have; as a matter of fact, it might be difficult to ensure an efficient enforcement of Article 28(2) of the USD and effective cooperation procedures between “relevant authorities” if, in each MS, different requirements – court decisions or administrative decisions – are settled in order to request to undertakings providing public communications networks and/or publicly available electronic communications services to block access to numbers/services and to withhold specific revenues.

4.3 A minimum set of responsibilities should be given to “relevant authorities”

Article 28(2) of the USD provides that “relevant authorities” shall be able to require undertakings to block acess to numbers or services and to withold interconnection and other service revenues. In order to require those enforcement actions to be taken, designated national authorities are likely to be able to receive complaints. This will allow NRAs to inform relevant authorities of other MS of identified misuse and/or fraudulent practices.

A compliance survey by “relevant authorities” might also be performed by some authorities following complaints received reporting end-users being harmed by potential cross-border misuse or fraud, and the results of this could be shared.

If designated national authorities are made responsible for directly handling such complaints, investigation of potential arming services can be much faster and simpler, allowing prompt requirement of blocking and witholding of services revenues to be enforced. This requires ability to handle complaints received, including from end-users from other MS.

Particular procedures for classifying and handling cross-border complaints between relevant authorities should be established. These procedures could provide for an appropriate interlinking of institutions responsible for the clearing of consumer protection affairs, such as national and European alternative disputes resolution mechanisms, with other national institutions to ensure that complaints are relayed to the appropriate authority under Article 28(2) of the USD.

In response to the public consultation and within the scope of the responsabilities to be given to relevant authorities, although not strictly related to enforcement actions but to a prior stage, one of the stakeholders [(29)] added a relevant consideration. As it considers that an approach to implementing Article 28(1) that requires “open access“ to numbers and services would be likely to lead to an increase in fraud and misuse, it suggests that NRAs could start by authorising open access to internationally defined and managed numbering, such as managed by ITU-T, for PRS provisioning (or to provision other services accessible by any country, associated with geographic or non-geographic numbers) [(30)]. With these international numbers, users can recognise what they actually are accessing, decreasing the chances of misuse.

It considered that another alternative to “open access“ would be to open individual types of non-geographic numbers one-by-one on the basis of actual demand, while ensuring that the services comply with national regulations and taking into account the constraints indicated above.

The question of access to numbers and services is due to be considered under the BEREC 2011 Work Programme.

[(29)] European Telecommunications Network Operators’ Association (ETNO).

[(30)] Currently, formally established international services use international numbers defined by ITU-T, such as International Freephone Numbers, +800, International Shared Cost Numbers, +808, International Premium Rate Numbers, +979, International Personal Numbers for Universal Personal Telecommunications, +878.

4.4 Provision of information by undertakings to relevant authorities for monitoring purposes

As in a privileged position to obtain information from providers delivering services in a cross-border basis, to act to block fraudulent services and numbers being misused, undertakings providing public communications networks and/or publicly available electronic communications services should co-operate with “relevant authorities” against fraud and misuse.

They could be enforced to provide to designated authorities, upon request, relevant data allowing the identification of providers with whom they have agreements (e.g., in a PRS context, platform providers, content providers…). This could facilitate NRAs to investigate and apply the enforcement actions foreseen under Article 28(2) of the USD, if necessary.

On the other hand, undertakings could also be interested in cooperate in such a way, as they normally are the first to receive complaints when problems arise. They bear the cost of bad debts and refusals to pay, as well as the cost of preventive action, such as for monitoring personnel and/or systems.

Also, specific problems such as PRS fraud create bad publicity and damage to consumer confidence. There is an additional risk that the public will misunderstand what role the originating electronic communications service provider plays in the overall PRS picture and that it may be associated with the fraudulent behaviour. Even where end-users understand that referred provider is not at fault, they may question why they do business in such a way that opportunities for fraud arise. All this can represent an exposure to the brand name of the operator.

4.5 A minimum and common set of enforcement actions should be defined by MS

Most NRAs already anticipate to be empowered in order to be able to require to undertakings, at a national level, to block access to numbers. They underline, nevertheless, that regulation of assignment of numbering resources and blocking number procedures

should be clearly established in order to allow to conclude what type of powers they can call on.

A number of NRAs also expect to be empowered to require to undertakings, at national level, to withhold interconnection or other service revenues. NRAs anticipate, however, that this enforcement action will be implemented in different ways – in some cases, NRAs may request the bill issuer not to issue bills for the number concerned; in other cases, NRAs may require undertakings to withdraw the revenues and pay them back to end-users deceived...

Meanwhile, at this stage, no respondent NRAs said that they expected to have the ability to require undertakings to block services. This may be because some NRAs expect to have the ability to block numbers instead, which they consider adequate; because some NRAs do not yet have clear expectations about transposition; or because another "relevant authority" may be empowered to require the blocking of services instead.

These approaches suggest a level of uncertainty remains as to the set of sanctions available for NRAs or other designated authorities to require undertakings to apply, at this point in the transposition process.

Thus, the transposition at national level of the revised USD should be used to define a coherent set of sanctions to be available to all "relevant authorities" in order to provide a consistent level of consumer protection across MS. Whatever the national Governments' decision on that matter migth be, NRAs should be able to harmonise their approach within the powers that they are given.

For such purpose, it should be taken in consideration that:

- Under the wording of Article 28(2) of the USD, the relevant authorities may require undertakings to block access to numbers and services and withhold service revenues [(31)].

[(31)] While blocking access to numbers/services may only prevent future harm, requiring originating electronic communications service providers to withhold interconnection or other services revenues

- Transposition into national legislation should let “relevant authorities” know if they are allowed to choose between requiring blocking access to numbers or services, as suitable, or if blocking access to services should be required in specific circumstances only (for instance, one SMS short code can give access to different services, of which only one could pose a problem; in such circumstances, it seems proportionate to require only the blocking of the access to the service in question, if technically feasible);

- When it comes to blocking the access to a number/service, it should be considered where its implementation might be more effective: in the country where the call is originated or in the country where the number was allocated.

  This will depend in a great deal on the features and platforms used by providers. However, an effective enforcement action to be taken can be the one by which the relevant national authority of the MS where the number was assigned requires undertakings to block access to the non-compliant number/service. Thus, all communications to that number, whatever the origin of communications addressed to it, would be blocked at a sole point, avoiding fraud or misuse.

  However, the relevant national authority of the MS where the number was assigned, if analysing a request from a relevant authority from another MS to block the access to that number based on alleged fraud or misuse harming end-users in other MS, may not have the same definitions for fraud or misuse. Based on different definitions, the relevant national authority of the MS where the number was assigned may therefore refuse to take enforcement action.

  Thus, if it is desirable that actions be taken by the relevant authorities of MS where end-users were harmed when contacting fraudulent or misused numbers allocated in

---

can to a certain – limited – extent address harm already occurred. In several cases, interconnection and other services revenues are paid out in a certain interval (e.g. every 14 days). If a number is, for instance, blocked in the 7th day of the 14-day interval, withholding revenues could also apply to revenue for traffic generated in days 1 to 6 of the 14-day interval.

another MS, it could be possible, and perhaps more realistic, for those authorities to request all providers in their MS that originate calls to the number in question to block all calls to that number/service [32];

- When it comes to blocking a number/service, the method used for such purpose should also be considered. The allocation of non-geographic numbers is done in most European countries in blocks of numbers. However, in many countries, there is already the possibility of assigning numbers individually to the content provider, which then finds an access network provider to start operating the service.

  From a technical point of view, in the case of allocation of blocks of numbers, the simplest solution is the one in which the relevant national authority requires that the access to the entire group of numbers in which the non-compliant number is in to be blocked. However, by implementing that solution, relevant authorities should bear in mind that other numbers within the group that has been blocked, which are not fraudulent or being misused, will also be affected.

  In response to the public consultation, in the event that "open access" was required, one of the stakeholders [33] underlined the risk if network operators and service providers had to block huge ranges of numbers, including numbers not misused and geographic numbers. The most extreme measure would be to block entire country codes (as it already happens towards some small or developing countries were numbers, both geographic and non-geographic, are misused).

  Also concerning number blocking, or call barring, the same stakeholder highlighted the existence of national regulations to block adult content related numbers. Again, in the event that "open access" to all non-geographic numbers was required, it noted that there would need to be a guarantee and a clear common understanding of the

[32] There is already the possibility of using specific platforms to block the calls based on their origin – notwithstanding, there may be some technical difficulties in implementing this solution. It requires parameters such as the CLIP or, in its absence, the identification of the call origin based on the route of origin, which can be difficult in the case of international carriers.
[33] European Telecommunications Network Operators' Association (ETNO).

difference between adult content and other content. As there is no such guarantee in each country, operators would depend on the application abroad. In addition, it would be technically very difficult to implement adult call barring options which take account of all international numbering plans.

BEREC notes that blocking access to a particular number within a block of numbers is also possible, but can be more demanding, making it more difficult to manage such blocks. Notwithstanding, relevant authorities willing to evaluate this alternative should discuss it with national undertakings, in order to collect their views on its implementation or on the implementation of an equivalent solution, such as blocking access to numbers that are part of black lists.

The same stakeholder [34] added also another possibility, which is to investigate opening up services to non-geographic numbers one-by-one on the basis of real demand, making sure that the services comply with the national regulation and taking into account the identified constraints. In this way, there would be a greater means to ensure that national regulation is respected by the services that becomes accessible. Blocking access to large ranges of numbers can that way be avoided. Again, BEREC will address the issue of accessibility of numbers and services under Article 28(1) of the revised USD in the 2011 Work Programme.

Should the blocking be made in the MS where the call was originated, the problem may not be particularly relevant, as many of the undertakings at the origin will also start to allocate numbers unitarily. This should also be discussed at a national level with undertakings;

- Withholding of revenues should be specified, in order to make clear in what way(s) it can be executed, by whom, which revenues can be withheld and for how long.

Any provider intervening in a communication, especially a cross-border one, with or without legitimacy, can retain revenues from that, as payments between operators

[34] European Telecommunications Network Operators' Association (ETNO).

are from the origin to the destination of the communication. However, for the purpose of implementation of Article 28(2) of the USD, it could be easier if undertakings required blocking access to numbers/services for reasons of fraud or misuse are the same providers that will withhold revenues. Blocking access and withholding revenues would happen in the same MS and would be performed by the same providers.

On the other hand, even if harmed end-users refuse to pay for their communications to the originating electronic communications providers there will be revenues along the wholesale chain to be withheld, for connecting the call. Perhaps the originating provider has already been billed by the transit and content providers, which it would then try to recover from the end-user. Those payments could be stopped along the chain before they reach the fraudulent content provider.

In the event harmed end-users pay for their communications to the originating electronic communications providers, a solution should be found that does not prejudice the possibility of them being reimbursed, promptly, for the expenses incurred in paying terminating providers for access to fraudulent or misused numbers. A simple way to do that would be for the provider to withhold revenues and agree a form of refund with end-users.

Also, a solution should be found that treats equally all carriers involved in making communications to a particular number possible, in the event that they are not responsible for that number being misused or used in a fraudulent way, and have just fulfilled their role in communication, i.e. carrying the communication between its source and destination.

It should also be specified if interconnection revenues will be the only ones to be considered for the purpose of enforcement, or otherwise other service revenues will also be taken in consideration. If that is the case, given the fact that this is a sanctioning measure, a list of possible services should be clearly identified. Notwithstanding, one can assume that wholesale services are included under Article 28(2) of the USD.

- Whatever the terms by which the above referred enforcement actions are established, the liability incurred by each of the parties involved in the provision of cross-border services should be clearly defined. Originating electronic communications service providers and transit operators should not be held liable for third party illegal content, but may play an important role in implementing enforcement measures.

4.6 Practical cooperation mechanisms between "relevant authorities"

Any efforts to enable end-users to access all numbers provided in the Community, including non-geographic numbers, where technically and economically feasible, should be accompanied by steps to strengthen mechanisms between MS for action against "fraud" and "misuse".

A proposal on the establishment of practical or even informal methods of cooperation between NRAs, where they are the relevant authorities seems, at this stage, important. This could be to:

- Gather and share information on possible instances of "fraud" or "misuse", given that the non-compliant provider may be based in one MS and the effects felt in one of more other MS, perhaps including an 'alert' system;

- Work out practical handling of cross-border cases when the end-user is based in another MS from the relevant enforcement authorities – assessment and prioritisation against domestic issues, jurisdiction of relevant codes of practice.

- Define the relevant types, content and levels of evidence that should be shared. Here it is necessary to consider how to deal with questions like the possible confidentiality of consumer complaints or NRA dealings with companies in some MS;

- Consider the need for practical tools, like contact lists, forms to request assistance from another authority, cross-border complaint forms, common approaches to reporting case results, etc.;

- Consider the possibility of establishing a single point of contact to facilitate cross-border cooperation;

- Work towards identifying common priorities for enforcement cooperation.

Where the relevant authorities are NRAs, BEREC should be the platform for them to develop a consistent approach and make sure that the procedures are clear in case the situations described in Article 28(2) of the USD occur.

BEREC could also be available to open this platform to relevant authorities other than NRAs, for the required harmonisation among MS to be properly achieved, perhaps through the intermediary of the NRA in those particular MS.

Glossary of terms

Given the technical nature of some of these issues, we have provided a glossary of English terms and phrases frequently used in this Report to describe different topics:

BEREC: Body of European Regulators for Electronic Communications;

Consumer: any natural person who uses or requests a publicly available electronic communications service for certain purposes, which are outside his or her trade, business or profession;

End-User: means a user not providing public communications networks or publicly available electronic communications services;

Interconnection agreements: are aimed to set prices and conditions for interconnection between networks, including access to special services of fixed network (information numbers, freephone numbers, call forwarding, etc.);

Premium rate services: refers to services that are accessed by the use of a premium rate telephone number in which the caller pays a special premium rate that is above the normal tariff for voice calls or SMS communication between end-users. Examples of services are sports information services, games, popular voting (as opposed to electoral voting), chat lines and business information services;

VoIP (Voice over Internet Protocol): The generic name for the transport of voice traffic using Internet Protocol (IP) technology. The VoIP traffic can be carried on a private managed network or the public Internet (see Internet telephony) or a combination of both. Some organisations use the term 'IP telephony' interchangeably with 'VoIP'.

References

Directive 2002/22/EC of the European Parliament and the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive)

Regulation (EC) No. 2006/2004 of the European Parliament and of the Council of 27 October 2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation)

European Commission Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation {SEC(2007) 1472} {SEC(2007) 1473}

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Citizens' Rights Directive)

Regulation (EC) No. 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of European Regulators for Electronic Communications (BEREC) and the Office

Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ("Unfair Commercial Practices Directive")

Work Programme 2011 BEREC Board of Regulators, December 2010. Available at: http://www.erg.eu.int/doc/berec/bor_10_43_1.pdf

EC, DG SANCO, Consumer Markets Scoreboard (CMS) 3rd edition 2010, "Consumers at Home in the Internal Market". Available at: http://ec.europa.eu/consumers/strategy/facts_en.htm

Cullen International SA and WIK Consult GmbH 2005, “Study on pan-European market for premium rate services”, June 2005. Available at: http://www.cullen-international.com/cullen/cipublic/studies/paneuropeanmarket.htm

OECD 2006, “Report on the cross-border enforcement of privacy laws”, October 2006. Available at: http://www.oecd.org/document/25/0,3343,en_2649_34255_37571993_1_1_1_1,00.html

Electronic Communications Committee (ECC) within the European Conference of Postal and Telecommunications Administrations (CEPT), Recommendation (07)02 Consumer Protection Against Abuse of High Tariff Services. Available at: http://www.erodocdb.dk/Docs/doc98/official/pdf/REC0702.PDF

ITU, Misuse of E.164 numbering resources, available at: http://www.itu.int/en/ITU-T/inr/Pages/misuse.aspx

ITU, Recommendation E.156 on Guidelines for ITU-T action on reported misuse of E.164 number resources. Available at: http://www.itu.int/rec/T-REC-E.156-200605-I

ECC, Recommendation (05)09 on customer protection in case of misuse or unauthorized use of international E.164 numbering resources. Available at: www.erodocdb.dk/Docs/doc98/official/pdf/REC0509.PDF

ECC/CEPT, NaN Project Team Number Portability, CLI related deliverables, available at: http://www.cept.org/sc?frames=no&mid=B59A18D9-D936-41A4-9B87-AB06A38D4B3A&

International Audiotext Regulators Network (IARN): http://www.iarn.org/
Handbook of the Independent Audiotext Regulators Network (IARN), available at:
http://www.iarn.org/upload/Handbook%20NOV2008.pdf

Consumer protection cooperation (CPC):
http://ec.europa.eu/consumers/enforcement/index_en.htm

European Government CERTs (EGC) group: http://www.egc-group.org/

Rapid Alert System for Dangerous Consumer Products (RAPEX):
http://ec.europa.eu/consumers/dyna/rapex/rapex_archives_en.cfm

European Advertising Standards Alliance (EASA): http://www.easa-alliance.org/

Early Alert System (EAS): http://www.cept.org/EAS?frames=no&mid=9E6698BC-E5D4-4A17-AC77-8BCDF20DAA45&

PhonePay Plus Code of Practice, available at:
http://www.phonepayplus.org.uk/output/Code-of-Practice.aspx