



Article 28(2) Universal Service Directive: A harmonised BEREC cooperation process -

Consultation paper

September 2012

Contents

1.	Executive Summary.....	3
2.	Introduction	5
2.1.	Objectives of the BEREC cooperation process.....	6
2.1.1.	Short and medium term objectives	6
2.1.2.	Long term objective	6
2.2.	Effectiveness and efficiency – benefits of harmonisation	6
2.3.	Purpose of Article 28 USD.....	7
2.3.1.	Objective of Article 28 USD.....	7
2.3.2.	Direct and indirect consequences for consumers	8
2.4.	Operator and end-user incentives	8
2.5.	Previous work by BEREC on Article 28 USD	9
3.	Article 28(2) USD issues	10
3.1.	3.1 Article 28(2) USD	10
3.2.	Misuse/fraud for the purposes of Article 28(2) USD	10
3.2.1.	Circumstances where the provision is relevant.....	10
3.2.2.	Direct versus indirect end-user protection.....	13
3.3.	Relevant authority for the purposes of Article 28(2) USD	14
3.4.	Powers given to relevant authorities.....	15
4.	Questionnaires issued during course of project	17
4.1.	Summary of results of questionnaire on transposition of Article 28(2)	17
4.2.	Questionnaire on scale/scope of problem.....	17
4.3.	Summary of results of questionnaire on the scale /scope of the problem	20
4.4.	Outcome of questionnaires: why a common process is needed.....	21
4.4.1.	Expected results from a common process.....	21
5.	Common process	22
5.1.	Introduction	22
5.2.	Relevant Authorities and NRAs Article 28(2)	23
5.3.	The process	23
5.3.1.	Initiation of the process – reporting a case of fraud or misuse	25
5.3.2.	Action by NRA in destination country.....	27
5.3.3.	Role of NRAs in transit countries	28

5.3.4.	Complexities in the process	28
5.4.	Other considerations	29
5.4.1.	Confidentiality of information	29
5.4.2.	Removing any requirement under the process for relevant undertakings to block access to numbers and services and/or withhold associated revenue	30
6.	Practical implementation of process	31
6.1.	Impact of national process on BEREC process	31
6.1.1.	Timing.....	32
6.1.2.	Thresholds.....	32
6.1.3.	Withholding of revenue versus information gathering	35
6.1.4.	Current interconnection payment schedules and contracts	36
6.1.5.	Different circumstances where elements of process might be applied	37
6.1.6.	Forum for reviewing process and thresholds	40
6.1.7.	BEREC Office support	40
7.	Protective measures that could be taken by NRAs, operators and end-users	41
7.1.	Improving security	41
7.1.1.	Improving the protection of telecommunication systems	41
7.1.2.	Improving the detection of fraud and abuses	41
7.2.	Moving to a self-policing role by operators for efficiency.....	42
7.2.1.	Cooperation with police or other law enforcement in member states to discourage incidents	42
	Annex 1 – List of questions	44
	Annex 2 – Questionnaire on scope/scale of problem.....	45

1. Executive Summary

1. The 2009 EU regulatory framework has introduced a new version of “Article 28(2) of the Universal Service Directive”¹, hereafter referred to as Article 28(2). The revised provision establishes the requirement for EU Member States to “ensure that the relevant national 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 services revenues”. Neither of the terms “fraud” and “misuse” were defined within the USD. Different countries use different definitions for each of these concepts, and this complicates European application of this measure.
2. This consultation highlights the background to fraud or misuse and its potential impact on consumers through falling foul of instances of fraud or misuse, or through a potential lack of confidence in the integrity of numbers. This could impact on innovation and development of services at retail level as well as a concern around take up of innovative services such as soft switches for businesses and residential service. This can also result in a lack of confidence in smart phone applications which will therefore have an impact on users take up of innovative smart phone applications.
3. Section 4 provides an analysis of the responses by a number of operators in member States and other countries and shows that there are a variety of different views amongst operators as to the scale and scope of fraud or misuse, particularly, it would seem, between retail and transit operators. Operators with different business propositions (e.g. fixed and mobile retail as well as transit) were included as it was considered that these would have differing perspectives on the problem.
4. The consultation outlines a proposed BEREC process for cross border regulatory cooperation in the intervention by the regulators or other relevant national authorities² in cases of fraud or misuse. Explanations as to how the process will work in practice are given in section 5. It should be noted that the BEREC process recognises that the decision as to whether to intervene is a matter for the relevant authority in the country concerned. Nonetheless even if intervention at a national level is not undertaken, there remains an expectation of cooperation in respect of information sharing.
5. In section 6 the problems associated with cross border cooperation in this area as well as the challenges for regulators and operators when supporting the relevant national and cross border processes are addressed.
6. It is likely that one of the main effective long term approaches to resolution of the problem of fraud or misuse will require greater cooperation between regulators and operators, to better understand the always changing fraud mechanisms and develop ex-ante and ex-post measures which can be taken to fight against fraud and misuse. These

¹ “Universal Service Directive”, 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.

² This process is intended for use by NRAs, facilitating cross-border cooperation between NRAs and the “relevant authorities” designated for the purposes of Article 28(2).

measures should not be a substitute for the normal measures operators and users have to take in order to offer and use electronic communication services in a safe way.

7. The ability to withhold interconnection and or service fees is a powerful one but there may be difficulties associated with putting the necessary contractual terms in place, particularly where the contracts may have include operators that operate outside Member States and outside the jurisdiction of the relevant EU Directives. It is envisaged that commercial pressures can however resolve these issues with time.
8. Finally, it is recognised that awareness of the risks associated with the use of telecommunications and the measures that end users can put in place to reduce their exposure to these risks should be improved.
9. BEREC proposes to monitor the practical issues around the implementation of the process and review the process as necessary.

2. Introduction

10. With the new Regulatory Framework of 2009, former Article 28 of the Universal Service Directive (USD) was rewritten in a more detailed way and expanded. Whereas the old version only stipulated a Community-wide access to non-geographic numbers, taking into account the technical and economical feasibility, and the voluntary non-accessibility of a called party, the new Article 28(1) USD goes beyond that. It explicitly calls for the “relevant national authorities” to take all necessary steps to make sure that end-users can access and use both services using non-geographic numbers as well as all numbers that are available within the European Union. Consequently Article 28(2) covers the issue of possible fraud or misuse scenarios that might arise from such an “open access” requirement through the establishment of a specific obligation for EU Member States to “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 services revenues”.
11. The provision therefore requires Member States to enable the “relevant national authorities” to require telecommunication undertakings to be able to block access to numbers and services³ when justified by reasons of fraud or misuse. Similarly, such “relevant national authorities” must be able to require the withholding of interconnection and other service revenues.
12. In 2011, as the outcome of its first report on the revised Article 28 USD, “Report on Cross Border Issues”⁴, BEREC found that more in-depth work should be carried out on the issue of the current situation regarding the accessibility of numbering resources. The results⁵ were published in the 2nd quarter of 2012.
13. As a further result of the 2011 report BEREC decided that, as part of the 2012 Work Programme⁶, guidelines should be drafted to define the relevant procedures for collaboration between “relevant national authorities” on the issue of fraud or misuse. It was noted that these guidelines should also include the mechanisms of how BEREC can provide assistance to independent National Regulatory Authorities (NRAs) (upon their request) on issues related to fraud or misuse of numbering resources, as BEREC is required to do so according to Article 3.1(l) of the BEREC Regulation.
14. As this is an initial consultation paper, readers are invited to provide their views, either in response to the questions contained in this paper (and listed in Annex 1), or by providing more general comments.

³ See Recital 38 of the Universal Service Directive

⁴ [BEREC Report on cross-border issues under Article 28\(2\)](#), BoR (10) 62 Rev1

⁵ [BEREC Report on the current accessibility of numbering resources pursuant to art. 28.1 USD](#), BoR (12) 53

⁶ [2012 BEREC Work Programme](#), BoR (11) 62

2.1. Objectives of the BEREC cooperation process

15. These guidelines will set out a description of how BEREC and NRAs will work together to address cross-border fraud or misuse of electronic communications. The document will also set out a common understanding of fraud or misuse in the scope of Article 28(2) in section 3.2. It should be noted that these guidelines do not define national processes for the tackling of fraud or misuse but are intended to facilitate communication between relevant authorities to support their approach to tackling such cases.

2.1.1. Short and medium term objectives

16. The guidelines are intended to increase consumer protection within the EU by a closer and more harmonised approach of the “relevant authorities” in the different Member States. The BEREC process could complement the national process implemented in order to comply with the requirements provided for in Article 28(2) and will contribute to the development of harmonised and efficient best practices at EU level. A quick and effective response by these authorities, harmonised at EU level, is necessary to support consumers who have already been affected by fraud or misuse scenarios. In addition, the timely blocking of numbers and services will also hinder a specific scenario from further harming any consumers in the future and protect operators affected by fraud or misuse cases.
17. The timely withholding of interconnection and other service revenues through the appropriate implementation of these guidelines is probably the most efficient tool to tackle fraud or misuse. Money flows will be interrupted, so the financial benefit of fraudulent behaviour and misuse can be minimised. This loss of illegitimate profits will reduce the incentives and therefore instances of fraud or misuse. In addition, the positive effects of close and efficient cooperation between the “relevant authorities” may lead to the better identification of the perpetrator, thus increasing the opportunity for successful prosecutions.

2.1.2. Long term objective

18. Article 28(2) establishes a general requirement for Member States and relevant national authorities in the context of fraud or misuse cases which has to be implemented. In the long run, one of the possible effects of the implementation of these BEREC guidelines is intended to progressively minimise the role of the “relevant authorities” regarding the fighting against fraud or misuse. They are intended not only to raise awareness among consumers but also among operators as well. If the providers of public communications networks and services realise that a common approach will result in a more effective and efficient provision of their services, then the enforcement role of the authorities may be progressively supplanted by commercially negotiated contracts and interconnection agreements.

2.2. Effectiveness and efficiency – benefits of harmonisation

19. These guidelines include for the purpose of the implementation of the Article 28(2) BEREC process a common understanding of the terms “fraud and misuse” as well as of the “relevant authority” and of the powers that should be given to these authorities. Whilst these terms are not specifically defined in the USD, such a common understanding of these basic terms is essential for a successful implementation of Article 28 (2).

20. A harmonised BEREC approach, which defines some, but not all, of the conditions under which NRAs may take action, will ensure that, taking into account the different national transpositions, such action can be started without any undue delay.
21. Such an approach will make sure that information can be forwarded in a much faster and reliable way; thus a common database of contact points of each “relevant authority” is necessary.
22. This approach will ensure that information is not only communicated in a timely manner, but also that the *appropriate* information is shared among the “relevant authorities” involved. This will increase efficiency – as delays can be avoided – as well as effectiveness – as the right measures can be taken based on the information available.

2.3. Purpose of Article 28 USD

2.3.1. Objective of Article 28 USD

23. The 2009 EU regulatory framework has introduced a new version of Article 28(2) of the Universal Service Directive¹. The revised provision establishes the requirement for EU Member States to “ensure that the relevant national 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 services revenues”.
24. In accordance with recital 46 of 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.”
25. As mentioned in BEREC’s 2011 “Report on Cross-Border Issues”⁴, Recital 38 of the “old” Universal Service Directive pointed out that “access by end-users to all numbering resources in the Community is a vital pre-condition for a single market”. According to the European Commission the 2007 proposal for the Review was intended, among others, to “strengthen certain consumers’ and users’ rights” – but also to ensure that “electronic communications are trustworthy, secure and reliable and provide a high level of protection for individual’s privacy and personal data”. The objective of Article 28 USD represents this objective that consumer rights are experienced across the single market in the field of cross-border communications that use numbers and services of all Member States. However, since cross-border accessibility might entail a higher risk of fraud or misuse, Article 28 also includes the specific requirements with regard to fraud or misuse cases so that ensure that these consumers’ rights can be safeguarded and defended. The consequences of not intervening in cases of fraud or misuse might harm the single market and damage these rights as well as the trustworthiness, security and reliability of electronic communications.

2.3.2. *Direct and indirect consequences for consumers*

26. Article 28 is included in Chapter IV of the USD, which is specifically dedicated to the protection of electronic communications end-users interests and rights. Apart from the obvious effect on consumers of fraud or misuse – financial losses – a lack of intervention might result in other consequences as well:

- As experienced in other cases before, fraud or misuse might harm the integrity of the National Numbering Plans. Once certain numbering ranges, especially those used for premium rate services, become linked with fraud or misuse, consumers stop using these numbering ranges. This might lead to the discontinuation of legitimate and innovative services that also use these very numbers. The NRA⁷ could, in the extreme, be required to close such a numbering range, resulting in the waste of a scarce resource.
- The overall quality of services offered would suffer if no mechanism is introduced, that makes sure that the “relevant authorities” are able to go after any attempt to commit fraud or misuse. Only if these authorities can work together on cross-border issues in a efficient and effective way to require the blocking of services or numbers as quickly as possible, consumers can be sure that the services they want to use will work properly and reliably.
- The existing charging systems might not be trusted anymore, once incorrect billing information has lead to an increased level of consumer complaints. Thus some services might not be offered anymore, which would lead to a smaller choice of services for end-users.
- As fraud or misuse usually results in additional costs not only for consumers, but for operators and service providers as well, undertakings might be forced to increase tariffs to recover these costs. Consequently consumers would suffer twice from fraudulent behaviour.

2.4. *Operator and end-user incentives*

27. The implementation of a BEREC process across Member States, together with cooperation from those relevant authorities (where different from the NRA) will help create an environment where a balance between the protection of end-users and operators can be struck. This will also help ensure that the correct incentives for both consumers and operators are achieved, ensuring the most efficient implementation of the measure. These incentives apply at all parts of the communications chain. At the retail level it is important to ensure that operators put in place efficient systems and processes to detect and handle fraud and ensure sufficient end-user protection. At the interconnect/transit level, the identification and management of fraudulent traffic through networks should ultimately be managed on a contractual basis. For terminating operators, due diligence should be taken in respect to the termination of potentially fraudulent calls. At the end-user level, appropriate security measures should be put in place to protect terminal equipment from outside misappropriation. Section **Error! Reference source not found.** sets out further detail on the issues that end-users and operators should consider in this context.

⁷ According to Art 10 of the Framework Directive, NRAs MS shall ensure that NRAs control the granting of rights of use of all national numbering resources and the management of the national numbering plans.

Question 1: Are there other incentives or issues that will impact end users and/or operators that should be considered by BEREC? If this is the case, please propose and explain such incentives or solutions.

2.5. Previous work by BEREC on Article 28 USD

28. Since the introduction of the revised Universal Service Directive BEREC has published two reports on Article 28:

- A “Report on Cross-Border Issues under Article 28 (2) USD”⁴, and
- “BEREC Report on the Current Accessibility of Numbering Resources Pursuant to Article 28 (1) USD”⁵.

Results from both reports have been taken into account in on this report.

29. As in the course of the report on cross-border issues the possibility of an increase of cases of fraud or misuse due to the Article 28(1) requirement for an “open access” to numbers and services was mentioned, the “BEREC Report on the Current Accessibility of Numbering Resources Pursuant to Article 28(1) USD” was added to the 2011 Work Programme. This report came to findings such as that

- whilst on the basis of the information gathered from some stakeholders, there might be a perceived lack of demand for a cross-border accessibility for all numbering ranges, this perception should not overlook the policy objectives established in the Directive 2002/22/EC as amended by Directive 2009/136/EC;
- more transparency could be introduced, e.g. on tariffs or charging models;
- guidelines on Article 28(2) should be taken into account by any further work on cross-border accessibility of non-geographic numbers;
- problems like fraud or misuse should be dealt with, especially in an international environment.

30. For this report BEREC conducted a survey among NRAs to identify situations where cross-border issues might arise, to find out how such issues are handled by NRAs and to understand which challenges NRAs might face as the “relevant national authority”.

31. BEREC came, among others, to the conclusion that the lack of an explicit definition of the terms “fraud and misuse” within the USD might hinder a harmonised application of Article 28 USD at EU level as such definitions would be subject to the relevant national transpositions. Thus a coordinated approach and practical cooperation mechanisms between “relevant authorities” may be elaborated. The same applies for the term “relevant national authority”, which in many cases might be the National Regulatory Authority for electronic communications, but, depending on the transposition of the Directive into national legislation, could also be another authority or even several authorities.

32. This process is intended for use by NRAs, facilitating cross-border cooperation between NRAs and the “relevant authorities” designated for the purposes of Article 28(2).

33. This report found that, in order to fulfil their duties according to Article 28(2), the “relevant national authorities” should be given a minimum set of responsibilities which enables them to block access to numbers or services in cases of fraud or misuse.

3. Article 28(2) USD issues

3.1. 3.1 Article 28(2) USD

34. The Citizens' Rights Directive 2009, introduced a new paragraph 2 to Article 28 Universal Service Directive, which established enforcement powers as a counterbalance to cross-border access to numbers or services. The provision deals with cases where enforcement powers are justified by reasons of fraud or misuse, and reads as follows:

"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 services revenues."

3.2. Misuse/fraud for the purposes of Article 28(2) USD

3.2.1. Circumstances where the provision is relevant

35. Article 28(2) does not provide a specific definition of the terms fraud or misuse. Therefore the scope of application of the provision is left open for implementation in the Member States. Situations covered by Article 28(2) include cases where providers involved in a call or other service are located within one single Member State as well as cases where providers are located in different Member States or beyond EU borders. Generally speaking, the scope of Article 28(2) is not necessarily limited to cross-border situations, although the present Guidelines have a more limited scope aimed at cooperating in cross-border cases.
36. Looking at the implementation by the Member States, most respondents confirmed that the implementation of Article 28(2) into national law has been made by means of literal transcription of the USD text. Further, no specific definition of fraud or misuse has been included in the legal provisions in most cases.
37. The UK's Communication Act 2003 states that "a person misuses an electronic communications network or electronic communications service if (a) the effect or likely effect of his use of the network or service is to cause another person unnecessarily to suffer annoyance, inconvenience or anxiety; or (b) he uses the network to engage in conduct the effect or likely effect of which is to cause another person unnecessarily to suffer annoyance, inconvenience or anxiety" (no definition of fraud is provided). This definition was however not developed in the context of Article 28(2) as it was in place prior to the Directive.
38. In Latvia, fraud is also defined in the context of using numbering as "*calling, routing or receipt of a call using services or numbering intended for end-users as a result of which useless or artificial traffic arises which may express as uniform calls in uncharacteristic amount or duration of connection for a user or as calls which are made by an end-user or equipment connected to a termination point exiting in Latvia or foreign states*" and misuse as the "*use of numbering intended for an end-user for the provision of services not included in the national numbering plan*".
39. In Finland, although no exact definition was provided fraud or misuse refer to situations where service seeks unlawful financial benefit by providing users with essentially false or

misleading information in marketing material and if fees resulting from the service accumulate on the user's communications service bill.

40. Some countries, however, have referred to examples or guidance provided in consumer protection Acts (Finland) or by criminal law provisions mostly related to fraud (Germany, Bulgaria, Slovakia, Switzerland and the UK).
41. As noted in the BEREC Report on cross-border issues under Article 28(2) issued in February 2011, it is in cross-border situations where more difficulties could arise in applying Article 28(2), as implemented into national laws.
42. A first approach to consider the scope of the notions of fraud or misuse can be taken by looking into the international applicable standards. According to ITU, a general definition of misuse in international numbers is provided in the following terms (ITU-T Rec-E.156-05/2006 and Suppl.1 (11/2007)):

“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 telecommunication service. 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 this Recommendation shall apply.

In cases where such misuse is deemed to be occurring nationally, then the issue should be raised with the relevant national numbering plan administrator. Issues regarding national numbering plans are outside the scope of this Recommendation.”

43. Also in the 2006 Recommendation on “Consumer protection in case of Misuse or Unauthorised User of International E.164 Numbering Resources⁸”, misuse in international numbers was understood to encompass “the use of international E.164 numbering resources i) non effectively assigned, often within CC 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 than those for which they were assigned”.
44. According to ITU, fraud, on the other hand, consists in the use of a number in the manner for which it was allocated but for the purpose of generating cash at the expense of the customer and/or operators.⁹
45. Further guidance was included in the questionnaire addressed to NRAs in preparation of the BEREC report on cross-border issues under Article 28(2), where fraud or misuse were deemed to have 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 communication services.

⁸ <http://www.ero-docdb.dk/docs/doc98/official/pdf/Rec0509.pdf>

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

46. The distinction between fraud or misuse can trigger difficulties, as evidenced in the ITU referred recommendation, which states as follows:

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

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

47. BEREC notes that this ITU definition of fraud is inconsistent with legitimate revenue-generating services such as premium rate services.
48. The scope of fraud or misuse in electronic communication services can also be inferred from existing practice at EU level. BEREC report on cross-border issues under Article 28(2) dated February 2011 includes the results of current practices. It encompasses examples of fraud or misuse related to revenue share numbers or services, including premium rate services as well as other practices falling under the category of misuse of numbering plans. Content issues (e.g. related to regulated or restricted activities, such as gambling) are not included in these Guidelines.
49. As these examples demonstrate, there is no single widely accepted definition for fraud or for misuse in this context. Given the jurisdictional differences, BEREC cannot define these individual terms. Nonetheless, a common understanding of what any reference (in this context) to the combined term “fraud or misuse” is needed to allow effective implementation of Article 28(2).
50. For this purpose, and for the purposes of providing guidance in the context of Article 28(2) and without prejudice to new forms of fraud or misuse that could appear in the future, examples of situations dealt with by operators and authorities that could qualify as fraud or misuse can be illustrated by the following examples:
- Use of numbering intended for an end-user for the provision of services not included in the national numbering plan of the relevant jurisdiction (for example auto-dialling)
 - The use of an unallocated number by a party without the consent of the allocating entity (for example short-stopping in the same country, in another EU country or beyond EU borders)
 - The use of a number by a third party to whom the number was not allocated, without the consent of the party to whom it was allocated (for example phone hijacking, or PBX hijacking)

- The use of an allocated number without obeying transparency obligations (e.g. omit or include an inadequate warning of the tariff, price announcement)
- Artificial inflation of traffic or causing artificial inflation of traffic. It refers to calls that:
 - are made, generated, stimulated and/or prolonged for the direct or indirect benefit of any entity operating, hosting or otherwise connected with a telecommunication service as a result of any activity by or on behalf of such entity.
 - result in a calling pattern which is disproportionate to the overall amount, duration and/or extent of calls which would be expected from a good faith usage; or an acceptable and reasonable commercial practice relating to the operation of telecommunication systems.

Examples include dialling numbers in the same country, in another EU country or beyond the EU borders. Typical examples of such practices encompass Private Automatic Branch Exchange (PABX) software modified by hackers to transit to foreign fixed, mobile and satellite premium rate numbers, scams designed to encourage consumers to call or text back (e.g. missed or short duration calls from international premium rates, non-geographic or other revenue sharing numbers) and scams that generate calls or texts from the customer without their direct action and/or knowledge (– e.g. dialler scams, smartphone applications, virus or other mobile malware, texts generated without the user's permission).

- Providing false information in the subscription or provision of electronic services, identity theft (concerning final customers, but also manipulation of network parameters), internal/employee thefts, or cloning cards are other situations which operators face on a regular basis.

51. A Relevant Authority may, unless precluded by national law, consider that “fraud or misuse” has occurred where an NRA or other relevant authority from another jurisdiction seeks cooperation in respect of an incident which is considered “fraud or misuse” in the Member State of the other jurisdiction. In this respect, Recitals 35 and 37 of the Framework Directive¹⁰ set out the need for cooperation between NRAs and the requirement to provide each other with the information necessary to apply the provisions of the Directives¹¹. This is further discussed in section 5.2.

3.2.2. *Direct versus indirect end-user protection*

52. As pointed out in the BEREC Report on cross-border issues under Article 28(2)4 issued in February 2011, 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, the revised framework 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.

¹⁰ “Framework Directive” Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services.

¹¹ It should be noted that this requirement is not limited to Article 28(2).

53. On the other hand, increasing the efficiency of cross-border enforcement is also 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 or 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.
54. Therefore, Article 28(2) and the implementing rules at national level can contribute to reducing or preventing consumer harm resulting from fraud or misuse and contribute to increasing the level of confidence that end-users have in cross-border commerce or services and higher end-user protection. Even in those cases where consumers are not directly impacted, reducing the extent to which operators are exposed to fraud or misuse (and therefore the costs associated with this exposure) should result in a corresponding decrease in the level of consumer harm.
55. The enforcement provisions of Article 28(2) should also prevent perpetrators of fraud or misuse from benefiting financially from their actions and ultimately have a deterrent effect.

3.3. Relevant authority for the purposes of Article 28(2) USD

56. As noted, the term “relevant authorities” is not defined in the USD. Indeed, the provision does not expressly refer to NRAs. Therefore, national implementation might appoint NRAs, but may result in the appointment of other entities. Section 5.2 sets out the difference between a “Relevant Authority” and an NRA in the context of this process. For the purposes of preparing these Guidelines, a questionnaire on transposition of Article 28(2) was sent on 23rd March 2012 to BEREC Contact Network members and observers.
57. The majority of the Member States that have fully implemented Article 28(2) have appointed the NRA as the “relevant authority”. There is a small group of countries where the “relevant authority” is judicial¹² (although the first referring entity may be the NRA, as in the case of France) and a few cases where the relevant authority is the one entrusted with consumer protection matters¹³.
58. In one case¹⁴ there has not been any specifically designated authority.
59. Some countries have referred to the role of police in fraud cases considering its criminal nature¹⁵ and others have mentioned the role of the NRA with regard to the management of numbering plans which are entrusted to them in several EU countries¹⁶.
60. Therefore, as a preliminary remark, for the purpose of coordination between the relevant authorities in cross-border cases and considering the status of the transposition in the

¹² This is the case of Bulgaria, France, Lithuania, Slovenia and Belgium for cases of fraud (misuse is managed by the NRA).

¹³ This is the case of Finland and Sweden.

¹⁴ Portugal.

¹⁵ This is the case in for example Latvia, Italy, Lithuania, Romania and Norway.

¹⁶ The response to the questionnaire specifically addressed this issue in the case of Germany and of Switzerland. There may, however, be other countries where the NRA is entrusted with plan numbering management.

Member States described above, it appears that NRAs could constitute a first contact point in the context of cross-border fraud or misuse cases.

61. The results of this questionnaire are further described in section 4.1.

3.4. Powers given to relevant authorities

62. As indicated in section 3.3 above, most Member States have implemented Article 28(2) directly. Therefore, considering the text of the USD there are two means of enforcement in cases of fraud or misuse:

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

63. Overall, from the responses provided to the questionnaire, it appears that the majority of the Member States that have implemented Article 28(2) have given responsibility for the enforcement of this measure to NRAs¹⁷.

64. In some cases, the powers set out in national legislation target specific services, such as value-added services¹⁸ and the scope to block or withhold payments is limited. There are also countries in which the measures to be adopted must be temporary in nature¹⁹.

65. In some countries the decision on fraudulent behaviour is publicized by the relevant authority²⁰.

66. There is one example where the above-referred measures are also implemented by operators in interconnection agreements²¹ and in some cases intervention by the relevant authority is indeed not deemed necessary in view of the fact that issues on fraud or misuse are addressed satisfactorily by service providers²².

67. Beyond the current status and application of Article 28(2) in national law as reported in the responses to the questionnaire, generally, the relevant authorities have discretion in adopting the enforcement measures. However, some relevant factors in the decision-making process include gathering information from the operators on the calls as well as the assessment of the:

- interpretation of the seriousness of the fraud or misuse (including the level of financial harm incurred; any other forms of detriment; the nature of the behaviour);
- perceived likelihood of action having an effect; and
- range of regulatory action available in the circumstance.

68. Both measures (i.e. blocking numbers and requiring the withholding of revenue) will have different effects and achieve different goals.

¹⁷ In Portugal, no specific authority was designated as relevant and “more than one authority may require companies to block access to numbers or services”.

¹⁸ This is the case of Austria.

¹⁹ This is again the case of Austria, Finland, and Slovakia.

²⁰ This is the case of Czech Republic.

²¹ This is the case of Latvia.

²² This is the case of Denmark.

69. Blocking (either originating or terminating, or both) numbers on a temporary basis will have the effect of preventing further calls, allowing further investigation and time to resolve the circumstances of the fraud or misuse.
70. Withholding revenues on the other hand will reduce the financial exposure for end-users and operators in connection with the calls already made.
71. As dealt with more detail in section 5, cross-border cases of fraud or misuse can entail difficulties to make the referred enforcement powers effective. For this reason, the present guidelines intend to draw some common understanding on the manner NRAs or other relevant authorities shall cooperate in situations of fraud or misuse affecting two or more Member States.

Question 2: Are there other issues related to the provision that are not discussed in this section that should be considered by BEREC? Please give details about your suggestions.

4. Questionnaires issued during course of project

4.1. Summary of results of questionnaire on transposition of Article 28(2)

72. 28 countries replied to the questionnaire regarding the transposition of Article 28(2), including 24 EU members (Austria, Bulgaria, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom) and 4 non-EU members (Croatia, Montenegro, Norway, Switzerland). With a few exceptions of countries where full implementation was pending, most Member States had implemented Article 28(2) into national law and appointed the “relevant authority” for the purposes of this provision. The questions addressed were as follows:

- (i) status of implementation,
- (ii) detail as to whether or not the provision has been transposed directly (without amending the Directive’s text) ;
- (iii) indication as to whether a definition of fraud or misuse has been included (including its specific content);
- (iv) the organization designated as the “relevant authority”;
- (v) confirmation as to whether the NRA will have any responsibility regarding the implementation of Article 28(2); and
- (vi) indication as to whether the concept of fraud or misuse has been defined in national law independently from transposing Article 28(2).
- (vii) where no implementation had taken place at that time, the Member States were asked to provide an indication on the intended implementation (questions (i) to (v))²³.

4.2. Questionnaire on scale/scope of problem

73. BEREC issued a questionnaire to NRAs requesting that they seek input from a limited number of different types of operators in their jurisdiction to ascertain the perception these operators had regarding fraud or misuse. It was anticipated that operators may have different perspectives on fraud or misuse depending upon whether their main focus is on fixed line retail services (to end users, whether business or residential consumers), mobile services or wholesale transit services. This exercise was undertaken to assess whether there was a common understanding amongst operators and NRAs of the scale and scope of the problem and to get background information on the approach to detection and handling of fraud or misuse.

74. The list of questions, together with summarised answers can be found in Annex 2. 27 countries replied to the questionnaire including 22 EU Members (Austria, Belgium,

²³ Seven countries had not fully implemented article 28.2 USD at the time the questionnaire was submitted (Italy, Netherlands, Poland, Spain, Slovenia and other non-EU countries including Montenegro, Norway and Switzerland) although the information provided on the expected implementation did not significantly differ from the countries where implementation was completed. In one case (Hungary) article 28.2 USD was transposed into national law by establishing the right and cases where the service provider may impose restrictions in the subscriber services. It appears that there is no regulatory intervention in cases of fraud or misuse of numbering leading to blocking access to numbers/services or withholding payments.

Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Spain and the United Kingdom.) and 5 non-EU members (Croatia, Lichtenstein, Montenegro, Norway and Switzerland).

75. This questionnaire requested views on the scale (the number and the financial value) and scope (the type) of incidents of misuse or fraud from at least one fixed retail operator, one mobile retail operator and one wholesale operator from each country. Most of the NRAs provided answers as a summary of responses from operators, since operators asked for their responses to be treated confidentially. As a result of this, it is difficult to break out the comparisons between retail and wholesale operators and between mobile and fixed operators. Similarly respondents tended to have a very particular viewpoint, meaning that retail operators do not tend to have the same views as transit operators. The outcome of the data analysis therefore represents these varied opinions and different incentives. Nonetheless the information gathered yields some interesting results.
76. Overall, the responses show that while operators within the same countries had similar approaches to their handling of fraud or misuse, their understanding of the scope of fraud or misuse varied to a degree and their perception of the scale of fraud varied quite significantly. This variation was also seen to be the case from country to country.
77. Most of the interviewed operators have indicated that they use automated systems for detecting fraud or misuse. Those operators that stated that they do not use automated systems stated that they rarely had instances of fraud or misuse or that they considered that the fraud or misuse, when identified, required manual analysis. Operators that responded also stated that they employ manual processes in addition to automated processes where available.
78. Operators that have fewer interconnections for international transit and/or termination state that they have fewer cases of fraudulent calls or misuse on their networks (for example, 4-5 cases per year) compared with those who have more interconnections for international transit and/or termination (The range of cases which are detected is from 1 incident per month to incidents detected daily).
79. Some operators indicated that the detection of fraud or misuse is done in real time, but the most respondents indicated that typical length of time to detect fraud or misuse on its network is 24 hours, with some exceptions where the typical length of time lasts several days. This demonstrates that operators have the ability to react in a timely manner.
80. Operators have indicated different levels of the value of fraudulent activities: from 6 000EUR to 19 000 000EUR. Spain noted that mobile network operators seem to suffer from 40 to 140 times more in the annual monetary value than fixed network operators. Some mobile operators tend to include subscription fraud in these figures.
81. Most respondents were unable to estimate the overall monetary value of traffic resulting from fraud or misuse. Some indicated 0.5-2% of overall revenue while others used indicative monetary value (200 000EUR - 2 000 000EUR).
82. The percentage of fraud or misuse detected both at retail and wholesale levels differs among operators as well countries and even within countries itself (e.g. Slovakia). Most of respondents (Austria, Denmark, Latvia, Malta, Romania, Slovenia, Slovakia,

Switzerland and Norway) indicated that the majority of (50% - 90%) detected fraud or misuse either originates and/or terminates outside EU countries.

83. Overall operators responded that they are able to detect almost all types of fraud or misuse listed in the questionnaire, with some exceptions.
84. Some operators have reported that they are also able to detect fraud affecting mostly business fraud (for example, subscription fraud, pre-paid fraud, shops fraud etc.)
85. Operators typically block access to a particular number in the first instance when they detect fraud or misuse.
86. Many responses noted that the retail customer is not generally charged for the fraudulent traffic. In other cases customers are fully or partly charged, but that depends of the details of the particular case.
87. Most operators pointed that the standard of evidence required from either retail or wholesale customers is a reference to the relevant Call Data Records (CDRs) (which the operators will then investigate themselves) or a criminal complaint.
88. The patterns of fraud or misuse are varied, but some main trends remain - calls to some international PRS/special services ranges generally to common destination countries (EU/Europe – Austria, Latvia, Bosnia, Bulgaria, France, Croatia, the UK, Liechtenstein, Poland, Moldavia, Slovenia, Italy, Spain etc., and beyond the EU- Cuba, Somali, Africa, Sierra Leone, Chile, Zimbabwe, Congo, Cook Islands, Bahrain, Pakistan etc.).
89. The majority of operators explained that they have AIT clauses in national interconnection contracts which enable to withhold payments or block numbers.
90. Some operators reported to NRAs that they have a clause that allows them to block numbers in international interconnection contracts, but none reported that they are able to withhold payments in the international interconnection contracts.
91. The majority of respondents reported that they do not have provisions within their international interconnection agreements for the withholding of payments or blocking of numbers (for any reason).
92. Some operators have indicated they interconnect with one while others interconnect with up to 500 other operators for international transit and/or termination.
93. Most of operators responded that they are able to track the precise routing of an individual international call originating on, or transiting across, their network.
94. Responses confirm that operators usually share information/intelligence on fraud or misuse with other network operators in their country or abroad.
95. Some operators stated that they inform other operators (countrywide, mother branch companies) and some operators indicated that they share information with GSMA, ETNO, FIINA (Forum of International Irregular Network Access) and CFCA (Communications Fraud Control Association).
96. Some operators indicated that they share information on fraud or misuse with enforcement agencies in their countries. Typically they share information with the NRA or police to support cases of investigations in individual cases.

97. Those who replied no, remarked that such information is only shared if legally permitted and necessary, as in many cases legal prosecution of fraud or misuse is very time consuming and often unsuccessful. Thus the operator rather focuses its activities on the detection of fraud or misuse and on trying to make such activities unattractive for those trying to commit fraud or misuse.

4.3. Summary of results of questionnaire on the scale /scope of the problem

98. Most operators use automated systems for detecting fraud or misuse. The typical length of time taken to detect fraud or misuse in operator's network is 24 hours, with some exceptions, which can last several days. Notwithstanding the foregoing, companies with few interconnection agreements and less turnover tend not to have automated systems and therefore the detection of fraud or misuse is conducted using a manual process which usually takes more time²⁴. The practice²⁵ shows that the most operators are able to track the precise routing of individual international calls within their own network (incoming traffic and outgoing traffic) but up to the closest carrier or partner.
99. NRAs suffer from a lack of information because some operators decline to provide information due to confidentiality reasons, or in some cases provide incorrect information. In other cases the incidents of detected fraud or misuse originate or terminate outside EU countries where laws, legislation and cooperation differ from national or EU principles. Transit operators are uninterested in the prosecution of fraud or misuse as they are not originating or terminating traffic and the prosecution process is time consuming.
100. Some operators require an extended period of time to gather and share the necessary information, and this can prolong delivery of information to relevant authorities and operators.
101. Some operators may directly contact (via e-mail or official letter) the national or foreign NRA providing the necessary information (identification of connection chain) and blocking access to specific numbers or services. However as previously noted that the NRA is not always the relevant authority.
102. Other than NRAs, court, police or some other authorities may also be involved in fraud or misuse cases.
103. The responses²⁶ of operators indicate that the standard evidence of fraud or misuse of numbers usually are CDR (call data records) or log files. Some operators have mentioned that declaration or some kind of statement provided by the operator is enough for them to block access to numbers or services and withhold payments, but some operators need the report from police or other law enforcement authority.
104. Obviously to obtain a report from police or other law enforcement (relevant) authority is time consuming and during this lead time (while operators receive the report of fraud or misuse (from operators and/or law enforcement (relevant) authorities)) some of the payments of fraudulent calls could be made. Also, some authorities may be unable to disclose information and/or documents to "relevant authorities" during the course of their

²⁴ Responses to the question 1 – 3 (Questionnaire on international scale & scope of fraud or misuse of numbers).

²⁵ Responses to the question 16 (Questionnaire on international scale & scope of fraud or misuse of numbers).

²⁶ Responses to the question 11 (Questionnaire on international scale & scope of fraud or misuse of numbers).

investigation. Unfortunately the withholding of payments is one of the few effective deterrents to fraud or misuse. And if at least one operator in the connection chain has made a payment there is at least one who benefits from the payments of fraudulent calls.

4.4. Outcome of questionnaires: why a common process is needed

105. Many practical difficulties have been experienced by NRAs when trying to implement Article 28(2). Such difficulties include a delay in reporting the fraud or misuse, resulting in payments being made, repeat instances of issues with the same customer, the practical difficulties associated with contacting regulatory authorities outside the legal framework of the EU, operators declining to provide information, providing incorrect information or taking too long to provide information.

4.4.1. Expected results from a common process

106. The previous discussion sets out some of the complexities that will be encountered when implementing a process to block access to numbers or services and to require the withholding of interconnection payments.

107. The implementation of a common BEREC process will streamline communication, improve the timelines of communication, and ensure that all NRAs are familiar with the types of information needed and the basis under which these are required.

108. Usually the harm associated with fraudulent calls falls on end-users and most of the responses²⁷ to the questionnaire suggest that retail customers are not usually charged for such fraudulent traffic, although in some cases customers are charged dependent on the details of the particular case. Where an operator has a financial exposure because it is unable to recover its costs, it may be appropriate that the NRA or relevant authority takes action to minimise that exposure.

109. These guidelines seek to establish a common process for the initiation of a case, how the circumstances of a case and a request for assistance will be communicated to relevant NRAs, and how the initiating NRA should manage the end to end process (including practical issues of cooperation between NRAs, harmonized platform which contains databases of details of (possibly) fraudulent cases, contacts of relevant authorities in each Member state etc.).

Question 3: Do the responses received and presented by BEREC represent an accurate reflection of the situation as experienced by operators and end users across Europe? Are there further aspects that should be considered by BEREC?

²⁷ Responses to the question 10 (Questionnaire on international scale & scope of fraud or misuse of numbers).

5. Common process

5.1. Introduction

110. This section sets out a common process for cooperation between relevant authorities in Member States in cross-border cases of fraud or misuse covered by Article 28(2) of the USD (referred to as ‘the process’).²⁸
111. There are three main objectives of the process: to protect the interests of consumers, to protect the interests of operators and to prevent perpetrators of fraud or misuse from benefitting from their behaviour. Preventing benefit from misuse or fraudulent behaviour should have the effect of reducing fraud or misuse and therefore further protecting consumers and operators. Such a process between NRAs will also have a positive outcome on operators, which have to dedicate increasing resources to detecting/preventing fraud situations.
112. The process is built on an understanding of how coordination and cooperation between relevant authorities in cases of fraud or misuse can be used to achieve this objective. The aim of the process is for all national regulators of EU Member States to ensure that the relevant authorities responsible for applying the powers in Article 28(2) USD in their country are encouraged to participate in a common cooperation process when dealing with cross-border cases of fraud or misuse.
113. The process facilitates the sharing of information and the issuing of requests for action in identified cases of fraud or misuse in an efficient manner. It seeks to balance effectiveness in achieving its objective with an appropriate level of intervention, and aims to implement measures that are quick to initiate and progress to a satisfactory outcome.
114. The process is designed to be workable across EU Member States (and ideally beyond). It ensures that relevant authorities in Member States:
- i) have an agreed common cross-border cooperation process to use in cases of fraud or misuse that complements their national processes;
 - ii) can access information on the appropriate contacts in other Member States in order to forward requests for information and/or action when required – and that the contact will be informed of the process and ready to act as appropriate; and
 - iii) can accommodate variations in implementation of Article 28(2).
115. The type of behaviour that might constitute fraud or misuse under the process is set out in section 3.2.
116. Article 28(2) USD refers to the requirement on Member States to ensure that relevant authorities can take the action set out. Commonly, the relevant authority to require the blocking of access and/or withholding of revenue in cases of fraud or misuse under Article 28(2) USD is the NRA. However, as set out section 5.2 below, other authorities (such as the police or relevant government department) may be considered as the relevant authority by some Member States.

²⁸ Cases of fraud or misuse of numbers or services within national borders are not covered by the process.

5.2. Relevant Authorities and NRAs Article 28(2)

117. These Guidelines pursue the goal of providing cooperation tools in cross-border situations that may arise in the context of frauds and misuse affecting operators located in more than one country. Specifically, the present section intends to provide information on the implementation of article 28(2) USD in the Member States and to illustrate cases that can be included within the scope of the common understanding of fraud or misuse and which can trigger the action of the “relevant authorities” in accordance with article 28.2 USD, which could be of particular relevance in EU jurisdictions where regulatory activity on frauds and misuse has been so far scarce.
118. Nevertheless, it is considered that, in general, the orchestrators and coordinators of the process will need to be the NRA in each Member State regardless of whether it is the designated relevant authority. This is due to the telecoms sector know-how and their experience in dealing with such situations. In contrast, other authorities, such as the police or judicial authorities in the countries where these are entrusted with the implementation of Article 28(2), are unlikely to be in a position to coordinate the detail of the process developed by regulators. In addition, actions taken by an NRA or other administrative authority to put a halt to a situation they feel falls within the remit of Art 28(2) may be independent from actions taken by judicial or other authorities under criminal law provisions. Therefore, NRAs are likely to be the national points of contact for the process and are referred to as such when describing the process in this section. Further, their participation as members of BEREC undoubtedly contributes to facilitate coordination and contacts. For the purposes of the present section reference to relevant authorities can be identified with the term NRAs.
119. NRAs at each stage of the process have discretion on a case-by-case basis as to whether to take action within their jurisdiction and, if so, the nature of that action.
120. Nevertheless, there is an expectation of cooperation between relevant authorities in line with the process described in this section, even if an NRA chooses not to investigate or take action in its own country.
121. For the purposes of preparing these Guidelines, a questionnaire on transposition of the Article 28(2) was sent on 23rd March 2012 to BEREC Contact Network members and observers. This is further discussed in section 4.1. The indications provided for in the present Guidelines do not prejudice the possible criminal actions or proceedings that may result from misuses or frauds, in accordance with the applicable rules in each EU jurisdiction.

5.3. The process

122. The process has a number of phases and roles for relevant authorities according to the particular circumstances of the fraud or misuse. The number of NRAs and countries involved will also vary according to the case, although these will generally be limited to countries where the calls involved originate and terminate. In some cases it may be necessary to consider the countries where traffic has been transited.
123. The process is illustrated in Figure 1 below. It is based on a scenario of a fraud or misuse originating and reported in Country 1, the relevant calls being transited by two different operators in Countries 2 and 3, before terminating with a fourth operator in Country 3.

124. In general, the process is instigated, coordinated and led by the NRA in the country where the fraud or misuse originates, and in fact the success of the process depends on this coordination and cooperation. The key actions for the NRAs involved are for:

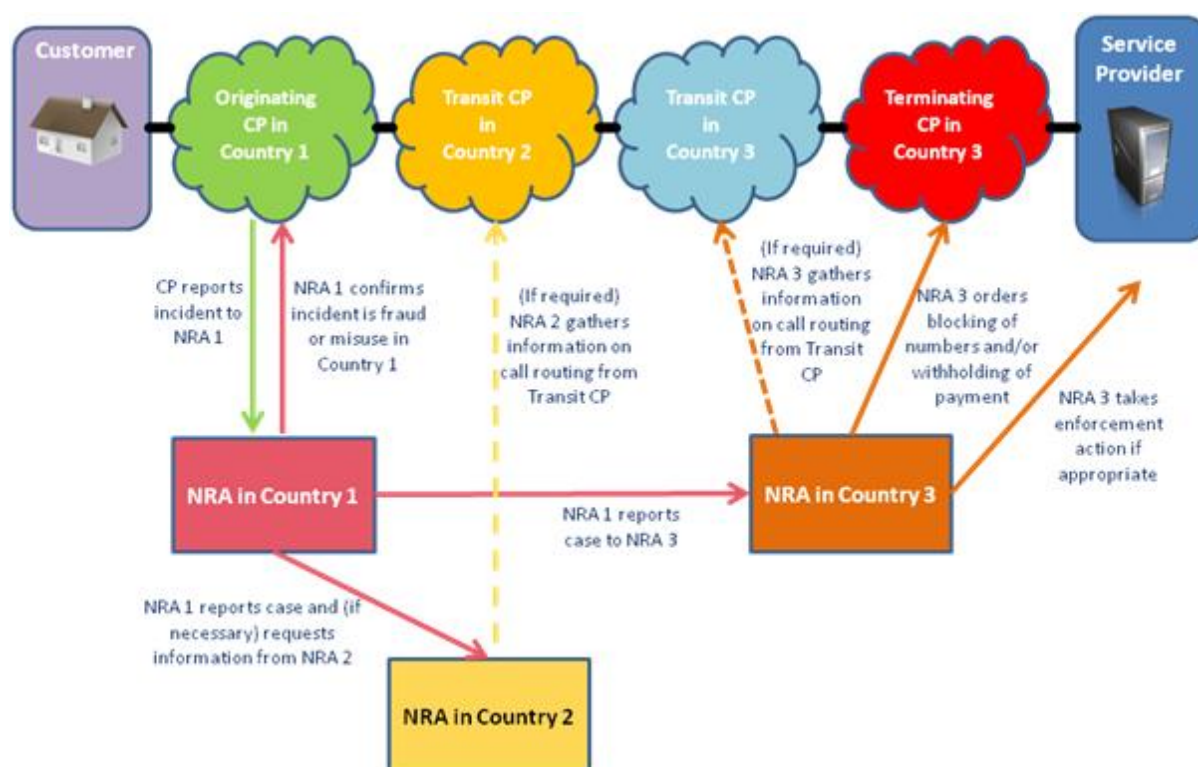
- i) the NRA in the originating country to consider what appropriate action it will take based on the details of the fraud or misuse. This action may include blocking access to numbers or services as well as requiring operators in that country to withhold relevant interconnect and other service revenue, but could also be any other regulatory action that may be appropriate;
- ii) the NRA in the originating country to inform the NRA in the destination country of the details of the case;
- iii) for the NRA in the destination country to consider appropriate action quickly; and
- iv) if the NRA in the originating country is to require that operators in its country withhold relevant interconnect and other service revenue, then that NRA should inform NRAs in transit countries of this action. This is to enable NRAs in transit countries to decide on appropriate action in their country of jurisdiction (e.g. this may include informing operators of the impact on interconnection and service revenues if withheld by operators in the originating country) and to provide any necessary support to the NRA in the originating country by obtaining information from operators as required.

125. The BEREC Office will facilitate the operation of the process. It will compile and maintain two reference databases for the purpose of applying the process. The first is a list of relevant authorities and NRA contact details in each Member State, with details of specific individuals to contact in cases of fraud or misuse under Article. 28(2) USD. This list will assist communications between relevant authorities and the coordination by NRAs (in general it is anticipated that the NRA in Member States will coordinate communications with the relevant authority where that NRA is not the relevant authority).

126. The second, confidential, reference database²⁹ is a register of cases of fraud or misuse reported under the process managed by NRAs in each country. This register will facilitate reviews of the effectiveness of the process undertaken from time to time. This process relies upon co-operation of NRAs for a successful result.

²⁹ This process and database will be subject to Article 20 of the BEREC Regulation (Regulation (EC) No 1211/2009 of the European Parliament and of the Council of 25 November 2009 establishing the Body of the European Regulators for Electronic Communications (BEREC) and the Office), which sets out that neither BEREC nor the Office shall publish or disclose to third parties information that they process or receive for which confidential treatment has been requested.

Figure 1: Overview of process for cooperation between relevant authorities under Article 28(2)



5.3.1. Initiation of the process – reporting a case of fraud or misuse

127. The action taken by the NRA in the originating country of the fraud or misuse (i.e. the NRA in Country 1 in Figure 1) is designed to:

- establish the facts about the case;
- report the case to the NRA in the destination country (that is the country from whose numbering plan the numbers called have been taken); and
- report the case to the BEREC Office.

128. The process is initiated by the NRA in the country of origination in response to the reporting of a case of fraud or misuse. The case may be reported to the NRA by the customer that is the victim of the fraud or misuse, by the operator serving that customer, by another operator in the communication chain or by another official body (e.g. the police).

129. In particular cases, the process may be also initiated by the NRA that is different from that of the origination country, specifically if the reporting of a case of fraud or misuse comes from an operator. In fact, operators have their methods to detect fraud or misuse and possibly also in cooperation among them at least at national level.

130. The NRA will confirm the facts of the case with the customer and/or the operator to an appropriate level, taking into account the potential need for urgent action. As part of this process, the NRA will verify that any cases of fraud have been reported to the police (if stipulated by national legislation).

131. It is the role of the NRA in the country of origination to establish whether, in its opinion and in accordance with its legislation, the case comes within the scope of fraud or

misuse covered by the process.³⁰ This decision will be based on the NRA's assessment of the level and nature of harm caused and on the proportionality and appropriateness of taking action. That action may include requiring relevant undertakings to block access to the numbers and service and/or withhold associated revenue under the process. Alternatively, the NRA may decide that other causes of action are more appropriate, including contacting other NRAs on a more informal basis to share information without requesting intervention. It remains at the discretion of the NRA not to take any action.

132. The NRA that initiated the process will examine the numbers called in the case and determine from which country's numbering plan they are taken (or, in some cases, the relevant service provider, such as Inmarsat). The country or countries identified will be considered as the destination countries for the termination of the calls unless contrary information comes to light as the process proceeds.³¹ The NRA of the destination country (i.e. the NRA in Country 3 in Figure 1) and the specific contact person is then determined through reference to the process contact list maintained by the BEREC Office. The NRA that initiated the process will then contact the NRA in the third country with the case information.
133. The NRA that initiated the process will inform the BEREC Office of the details of the case, including the telephone numbers involved and any action taken, in order for BEREC to include the details on its register of cases of fraud or misuse reported under the process. The BEREC Office should be informed as soon as this process is initiated and updated as new details or decisions are known.
134. The NRA that initiated the process has case-by-case discretion as to its level of additional involvement in the process (e.g. contacting transit NRAs and/or transit operators to attempt to trace the call flow from origination to termination). This may depend on the level of investigation that the NRA requires for its case assessment and the nature of action taken.

³⁰ See Section 3.2 for the type of behaviour that may be covered by the process.

³¹ Situations where calls to numbers from one country's numbering plan terminate in another country are considered in section 2.4.2.

135. In summary, the NRA that initiated the process may undertake the actions set out in the box below:

NRA in originating country (i.e. Country 1) needs to:

- Confirm the facts of the case
- Confirm that the case qualifies as fraud or misuse in the originating country (i.e. Country 1)
- Confirm whether the fraud or misuse is ongoing and if it has been reported to the police where necessary
- Confirm the quantity of money involved in the fraud or misuse
- Determine what appears to be the country of destination of the calls and report the case to the NRA in the destination country (i.e. Country 3)
- Determine the transit countries for the calls (i.e. Country 2). Depending on the circumstances of the case, report the fraud or misuse to the NRA(s) in the transit country(ies)
- Coordinate the responses from the NRAs in the destination and transit country(ies)
- Report the case including the called numbers and any action taken to the BEREC Office

5.3.2. Action by NRA in destination country

136. The action taken by the NRA in the destination country (i.e. the NRA in Country 3 in Figure 1) is designed to prevent the perpetrators of the fraud or misuse from benefitting financially from their behaviour.
137. The appropriate action to be taken by the NRA in the destination country will depend on the type of fraud or misuse that has occurred and will be at the discretion of the NRA in the destination country. The NRA will consider the facts of the case and determine, with reference to its national legislation and other relevant factors, whether it considers the case qualifies as one of fraud or misuse in this country and whether it is prepared to act in accordance with the process at the request of the NRA in the originating country.
138. If the NRA in the destination country agrees to consider taking action, it will need to supplement the information on the case provided by the NRA in the originating country in order to act. This additional information is likely to include identifying the terminating operator(s) for the relevant numbers and, if appropriate, the associated service provider. The NRA may also (at this point, or as a follow-up to the investigation) identify levels of call traffic from any other sources to the relevant numbers in order to determine the likely scale and sources of interconnection and other service revenues generated by calls to the numbers.
139. Different courses of action may be available to the NRA in the destination country. These may include invoking powers under Article. 28(2) USD³² to require relevant undertakings to block access to numbers or services and/or require the withholding of relevant interconnect or other service revenues. Other action may be taken depending on the powers at the NRA's disposal.

³² If the destination country is an EU Member State or the NRA (or other relevant authority) has similar powers to those provided for in Article 28(2).

140. Having considered the relevant courses of action, the NRA in the destination country should notify the NRA in the originating country or the NRA that initiated the process of how it proposes to proceed and report on any enforcement action that it has or intends to take. If action is taken, it should keep the initiating NRA informed of progress and developments. It should also notify the BEREC Office and report the outcome for recording in the register of cases of fraud or misuse reported under the process.
141. In summary, the NRA in the destination country may undertake the actions set out in the box below:

NRA in destination country (Country 3) needs to:

- Confirm whether the case qualifies as fraud or misuse in the destination country (Country 3)
- Identify the terminating operator (if relevant the Service Provider) for relevant numbers
- Identify levels of call traffic from other sources to the relevant numbers
- Consider an order to block access to the relevant numbers and services
- Consider an order to withhold interconnect and other service payments
- Report the outcome to the NRA in the originating country (Country 1)
- Report the outcome to the BEREC Office

5.3.3. Role of NRAs in transit countries

142. The role taken by NRAs in transit countries (i.e. the NRA in Country 2 in Figure 1) includes information gathering and sharing. Depending on the case and the actions of the NRA in the originating country, the role may also include requiring operators to block interconnection and relevant service revenues. The NRA in the transit country may, in certain circumstances, also require access to numbers and services to be blocked. However, this would not be the norm as blocking of access is more likely to take place in the origination and/or termination countries.
143. In cases where the sharing of revenue has been blocked in the origination or earlier transit countries, the NRA in the transit country should consider the impact on operators in the country of its jurisdiction and whether it should take any action. The thresholds for intervention (both those set for the process and for that country's national intervention) will be relevant for assessing the likely impact on operators and any decision to intervene.
144. The role of operators and NRAs in compiling information on the transit of the call will be particularly important in cases where the apparent destination country is not the country where the call actually terminates. This scenario is discussed in the next section.

5.3.4. Complexities in the process

145. There are a number of situations where the process described in sections 5.2.1 to 5.2.3 above has added complexities. These are described below.

5.3.4.1. Transit and/or destination countries are outside of the EU

146. The process has been devised to facilitate Member States in their implementation and application of the requirements in Article 28(2) USD and is based on the power to require

operators to block access to numbers and services and/or withhold relevant revenue in cases justified by reasons of fraud or misuse.

147. In cases where the NRA in the originating country finds that the transit or destination countries are outside of the EU, the NRA should still attempt to follow the process, which is based on a logical course of intervention to protect consumers from fraud or misuse. NRAs in Member States should be aware, however, that the range of action available to non-Member State NRAs may be different and may not include the power (or have a devised process) for requiring blocking of access to numbers and services or for withholding relevant revenue.

5.3.4.2. The numbers called are 'short-stopped'³³ or have not been allocated or assigned to an end-user

148. The NRA in the originating country will establish what it expects to be the destination country for the calls by determining the country from whose numbering plan the numbers have been taken. However, it may become clear following further investigation (generally after contacting the NRA in the apparent destination country) that the calls do not terminate in that country and are 'short-stopped' in another destination.
149. The NRA in the destination country may also find, following investigation, that the numbers involved have not been allocated by the NRA or assigned to an end user, and therefore should not be in use. In such a scenario, it is likely that the calls are being short-stopped in another country for call termination.
150. In both the above situations, the NRA in the apparent destination country may not be able to provide any information or identify relevant undertakings upon which to take action. The NRA in the apparent destination country should inform the NRA in the originating country of this situation.
151. In order to determine the actual country of call termination, the NRA in the originating country may attempt to trace the call flow from origination to destination by contacting the relevant transit NRAs to share information on the case. This may include requesting the NRA to gather information (either informally or using formal information gathering powers) to help determine the country of call termination.

5.4. Other considerations

5.4.1. Confidentiality of information

152. Due regard must be given to confidentiality requirements in each Member State if commercially confidential information, 'personal data' (as defined in data protection legislation) or communications data (as defined in legislation on lawful interception and data retention) is passed between NRAs during the tracking of call traffic. Each NRA will need to ensure that they act in accordance with their national legislation and EU law on the handling/disclosure of these types of information.
153. Relevant authorities may need to apply certain restrictions on the information shared with other NRAs, in accordance with Article 5(3) of the Framework Directive. For instance, national police, if involved in the process, may require specific aspects of information to remain confidential during investigation of the case.

³³ That is, the country from whose numbering plan the numbers are taken is not the destination country.

5.4.2. *Removing any requirement under the process for relevant undertakings to block access to numbers and services and/or withhold associated revenue*

154. If numbers and services that are subject to a requirement under the process for relevant undertakings to block access and/or withhold associated revenue are no longer associated with fraud or misuse, the NRA in the destination country may request that relevant authorities remove any requirements in their countries to block access and/or withhold associated revenue.

Question 4: Do you consider the proposed process to constitute a practical and effective method for NRAs to cooperate with each other in order to implement the requirements of Article 28(2)? Please explain your view with any suggestions you may have.

6. Practical implementation of process

6.1. Impact of national process on BEREC process

155. The proposed Berec process interfaces to national processes for implementation of Article 28(2). The details of the national processes may differ from country to country but their interface with the Berec process needs to be effective and efficient.
156. The national processes may envisage number blocking, revenue withholding or information gathering depending upon the circumstances of the incident under consideration. The Berec process is designed to support these options by facilitating communication and cooperation between Member States.
157. Whatever the national approach, and without prejudice to actions taken by national authorities in the different Member States for the transposition and implementation of the requirements provided in Article 28(2), the objective of the BEREC process is to standardise to the extent practical the interface requirements and processes between the various national processes of the relevant NRAs in cross-border cases of fraud or misuse, as described in the previous section.
158. A significant consideration is that in some Member States the NRA is not the "relevant authority" for some or all of the associated powers of Article 28(2). It therefore needs to be considered as to how the BEREC process will interface to "relevant authorities" where this authority is not the NRA. The two options considered are:
 - to communicate this process to the relevant authorities and involve them directly in the cross border process; or
 - to encourage NRAs to coordinate the communication between the relevant authority in their Member State and the NRAs involved in this process.
159. It is BEREC's view that to facilitate a cross-border process such as this will be most effective handled by NRAs, given existing experience of cooperation between NRAs. This does not preclude appropriate communications between NRAs from one Member State and a non-NRA Relevant Authority in another, but it is envisaged that for the initial implementation of a BEREC process the approach will be more manageable between Member States building upon the current BEREC structure and established contacts.
160. The required coordination between NRAs for Article 28(2) will involve gathering information, imparting information and inviting or requesting intervention by another Member State in the areas of blocking numbers or requiring the withholding of interconnection or service revenues.
161. In most cases the national process will involve gathering information from operators, whether the investigation is triggered by an incident in that jurisdiction or a request for assistance has been received from another NRA, to determine what action is appropriate and to communicate to the relevant operators within its jurisdiction what action is to be taken. Where a request for assistance from another NRA has been received the process for gathering information from operators will require information to be provided by the originating NRA and information to be returned to that NRA. Given the potential for several operators and several NRAs to be involved, in order to ensure efficient communication of information a standard format for the information exchange is desirable. This includes information such as originating and terminating numbers,

operator routing the traffic and call detail records (CDRs) for the calls being investigated. In addition sufficient information should be provided to demonstrate to the supporting NRA the basis for the initiation of a case by the requesting NRA. This information may for example include a confirmation that the incident has been reported to the local police (depending on national legislation), before action other than information gathering, is taken. There will be circumstances where this is not necessary, such as an incident impacting several end users which is being investigated as an own-initiative case by an NRA based on general complaints.

162. Another key impact of national processes on the Berec process is the national decision whether to intervene in respect of number blocking, revenue withholding or information gathering. As information gathering is a necessary requirement for tracking the path of calls and hence identifying operators in the chain this would normally be undertaken upon request. Where any aspect of the request, such as blocking revenue, is not being progressed in the country concerned this should be communicated to the requestor with a justification.

6.1.1. *Timing*

163. As one possible intervention is the requirement to withhold interconnection revenues across several jurisdictions, to come to this conclusion and effectively implement the process in the relevant jurisdictions the process must allow rapid decision-making, sufficient to allow implementation prior to payments being made. All these actions must be progressed with urgency as the timescale to intervene in interconnection payments is very short due to the nature of the relevant commercial contracts.
164. The national processes and the BEREC process must therefore support a timely response to information requests or requests for support and in that context agreed structures are required for communication. Once the initiating NRA launches this cross-border process, this NRA should notify other relevant NRAs and the BEREC Office that they have done so.
165. Given the importance of timing, which is discussed in section 6.1.4, it may be considered necessary by an NRA to make an interim finding in order to allow time for further investigation into the relevant incident. Following this investigation, the NRA may then make a final finding upholding its original interim decision, or, depending on the evidence received, rescind the original decision. The advantage of this approach is that it can put a hold on interconnection payments and service revenues for a period during which the investigation can continue, operators can be advised of the basis for the intervention and operators and other parties have time to make considered representations to the originating NRA.
166. The BEREC process and relevant national processes should facilitate this temporary intervention pending the conclusion of the investigation process by a Relevant Authority.

6.1.2. *Thresholds*

167. Since the introduction of Article 28(2) the experience of NRAs that have intervened in this area suggests that the resources associated with such investigations can be significant. Even given process developments for cross border cooperation it does not seem likely at this stage that intervention in every single case would be practical for NRAs and operators. For this reason, in this section we consider implications of

introducing as a BEREC non-binding guidance and without prejudice of transposition and implementation measures to be implemented by the relevant authorities to comply with the requirement established under EU law, a threshold below which it may not be practical for NRAs (or relevant authorities) and for the overall achievement of the objectives established in Article 28(2) to intervene.

168. The originating NRA should identify the charges the retail operator intends to apply to the retail end-user. This charge may be the normal retail charges for the calls or may be the wholesale charges which the retail operator intends to pass on, instead of the retail charges in this instance. With this information the requesting NRA can determine whether the incident falls within those thresholds used to determine whether in certain cases it would be proportionate to implement the actions envisaged under Article 28(2) (i.e. blocking of numbers and/or withholding of revenue).
169. It should be noted that Article 28(2) does not suggest that an NRA may require a retail operator to waive retail charges; however the level that an operator intends to charge may influence the decision as to whether the NRA wishes to take action under this process. If the retail operator intends to charge, or has already charged, the full retail price associated with the fraudulent traffic to the end user, the requesting NRA may consider it inappropriate to impose the full rigour of this process as the end user harm will result from these charges and will not be influenced by the application of the process. Requiring the retail operator to withhold revenues in those circumstances would result in the retail operator benefiting from the retail revenues without incurring wholesale cost. It is likely that the requesting NRA will consider it inappropriate to required withholding of interconnection revenue where this is the case since this may result in the retail operator benefiting from fraudulent revenue which would provide a disincentive to detect fraud at an early stage. However the NRA may decide to progress with respect to the investigation with a view to having the funds to the perpetrator withheld at the end of the chain.
170. Another reason an NRA may consider not intervening is in those circumstances where the impact on an end-user is below the threshold envisaged by this process, or the impact on a retail or transit operator is below the relevant threshold. This could result in an intervention along some of the communications chain, but not with some transit operators where the revenues have been diluted to an extent that intervention would be considered as disproportionate by the NRA. In the case of the payments to operators or entities near the end of the chain it may however still be appropriate to intervene to disrupt the payments to perpetrators of fraud or misuse.
171. One of the considerations of this process is that BEREC considers that the protection of end users is required because of their lack of awareness of the implications of lax security in the systems. In this context an originating NRA may take the view that a second incident with the same end user may not warrant an investigation or the threshold may be considered to be inappropriate given the awareness that the end user gained from the first incident. This may be appropriate for example in such cases where the end user has past experience of such fraudulent traffic and has not put in place any extra security.
172. Considerations into the establishment of a threshold include:

- If a high fixed financial threshold is set it will result in a number of end users being exposed to potentially significant cost and such a threshold will not act as a deterrent to perpetrators as they will still benefit from these incidents.
 - A possible alternative is that the threshold may be set by reference to the significance of an incident to an end user. This may be best characterised as the level of the cost of the fraud or misuse as a multiple of a typical monthly telecoms bill. If this simple approach is adopted, and if the incident relates to a user who would typically have a bill of several thousand of euro each month, the thresholds may again not act as a deterrent to perpetrators as they will still benefit from these incidents.
 - A combined approach which addresses the threshold in the context of end user harm, considering harm to be the relative impact against a typical telecoms bills for that end user, and also considers the threshold in the context of disrupting the more significant money flows to the perpetrator of the incident can be achieved through a combination of the fixed and variable thresholds. This approach would be a trade off between the distribution of values of incidents, the resources required in the NRA or other relevant authorities and operators to address each incident and the effort involved in any intervention.
173. The proposed BEREC approach, which constitutes a non-binding guidance vis-à-vis the NRAs or other relevant authorities in implementing Article 28(2) in the adoption of measures consisting of blocking numbers and/or withholding revenues and without prejudice of the general requirement provided for in Article 28(2), is therefore as follows³⁴:
- NRAs or other relevant authorities would normally act in cases where cross border cooperation is required if the charge to be applied to the end user exceeds €5,000. Where the charge to an end user is below this level an NRA would normally require cross border co-operation where the charge to be applied to the end user exceeds a factor of [3] times the normal bill but not if the charge was below €1,500.
 - Since Article 28(2) establishes a general requirement, it is within NRAs or Member States national relevant authorities' competence to intervene in cases that fall outside these thresholds. One possible example would be a situation where the form of misuse involved will be of a very low value to an individual user, however it could be applied to a significant number of end users and the aggregate amount may be significant. An example of this may be a PING call where users are encouraged to return a call through a short duration call appearing as a missed call on a mobile.
 - The threshold to be applied for transit operators is a matter for national processes and may be set at such a level that the administration cost of withholding revenues does not exceed the amount withheld. However, this threshold may not be relevant in the context of information gathering where the information may be needed to identify the end destination of the calls.
174. Note that in the context of the above considerations the charge to the end user (or previous operator) would be the charge that the operator intended to apply for the incident (either at the retail or at the wholesale level). In some cases it is also possible

³⁴ Other than regulatory intervention account is to be taken of other possible means to limit the incidence of frauds/misuse (e.g. commercial practices, specific consumer protection or technical rules).

that other forms of fraud or misuse may be perpetrated which do not entail a direct financial cost to the end user. A possible example of this could be a phishing incident.

175. It should be noted that the initial decision as to whether to act is generally taken by the NRA in the Member State where the incident that qualifies as fraud or misuse occurred. By the time the transactions have flowed through a number of wholesale carriers the financial elements of the charges will be reduced, potentially below these thresholds.
176. While the originating NRA may ask for information to be provided from an NRA of a transit operator and for revenues to be blocked, the national process of the transit operator's NRA may be such that they decide not to intervene in the context of revenue blocking, due to their views on thresholds but the NRA would normally seek to get the relevant information to enable the originating NRA to track the calls as a minimum. It should be noted that an NRA choosing not to intervene in respect of withholding revenues may result in an operator in its jurisdiction having to contractually make an out payment for the transit calls while being unable to collect the revenue for the calls from the operator in the earlier jurisdiction.
177. It is important to set these thresholds at a level that is sufficient to ensure that the end-user (particularly non-consumer end-users) are appropriately incentivised to take ample measures to protect their equipment and numbers from fraud or misuse. Simple steps, such as changing default passwords on server equipment, should always be taken. The national process for NRAs should include informing end users of the generic risks and the expectation that appropriate security measures are taken. In cases where the same end-user has been the victim of a second or subsequent case of fraud or misuse, but where no extra security measures have been put in place, it may be appropriate to set a threshold higher than that used for an end-user that has taken all reasonable steps to ensure security. However, as previously mentioned, NRAs may still wish to implement the procedure to gain information regarding the fraud or misuse and to disrupt money flows to the perpetrators.
178. Additionally, as suggested above the thresholds that apply at retail level should not be applied at a transit level, since it is likely that the traffic – and therefore associated charges – that leaves a retail operator will be distributed between many transit operators. This means that lower thresholds should apply at this level. On the other hand, it may not be appropriate to require the withholding of revenue below a certain level, particularly where the transactions costs borne by the relevant operator are in excess of the revenue involved. In these cases, since the main objective is to disrupt the money flow to the perpetrators, it may still be appropriate to require the withholding of revenue by the terminating operator (if known).

Question 5: Are these initial thresholds for retail operators and transit operators set at a realistic and practical level? Should other issues affecting whether NRAs initiate a case under this process be considered on a systematic, rather than ad hoc, basis? Please provide details on any proposals made.

6.1.3. *Withholding of revenue versus information gathering*

179. In cases where the originating NRA considers it inappropriate to require the withholding of revenue, it may still consider it appropriate to request information about the call traffic

from the retail operator with the intention of disrupting the money flow to the perpetrators of fraud or misuse.

6.1.4. *Current interconnection payment schedules and contracts*

180. Interconnection and service revenue payment schedules typically envisage 30 to 60 day settlement periods but these can be considerably shorter. In the event that an NRA requires the withholding of interconnection payments, such a decision needs to be taken in sufficient time to allow the operator concerned a reasonable opportunity to give practical effect to this requirement.
181. It is understood that interconnection agreements can operate on a “net settlements” basis, which means that an aggregate payment is made by the operator who, on balance, has terminated more traffic with the partner operator than vice versa. This makes it practically difficult for operators to withhold the revenue associated with certain call records, since the operator in question is *owed* a settlement payment by the interconnecting operator, rather than *owing* a settlement payment. In such cases, it may be appropriate for the originating NRA to require the relevant operator to nevertheless withhold the revenue and any discrepancy due to the net settlement approach would be identified as an incorrect settlement and accounted for appropriately. This should then trigger normal dispute terms in the relevant contracts. In practice it is hoped that operators will develop these contracts to put in place a more streamlined approach to handling the withholding of payments. This is a medium term goal of BEREC as it will reduce the burden on NRAs and operators in the operation of an Article 28(2) process.
182. It may not be possible in every case, and in particular in early cases to be totally effective in the objective to ensure the effective disruption of revenue to the perpetrators of fraud or misuse. The process will however aim to minimise any disproportionate impact on those operators carrying such traffic in good faith. This is best achieved if the flow of money is disrupted as early as possible in the chain of interconnection payments. A priority in the disruption of the revenues is to prevent the payments at the far end to the entity perpetrating or significantly benefiting from the Fraud or Misuse. It should be noted that this entity can be an operator, a service provider or an end user in some form of commercial agreement with a service provider or operator. An inability to disrupt the overall flow of money would not be considered as precluding the use of this process to the extent possible.
183. Experience has shown that some operators may have committed to contracts that do not permit the withholding of interconnection revenues, even if such revenues originate through the perpetration of fraud or misuse. In such cases the action should be taken to render such clauses ineffective through the use of Article 28(2) where possible.

Question 6: Are there other types of clauses found in typical commercial interconnection or other agreements that might influence the ability of operators to withhold interconnection revenues when required to do so by an NRA? Please provide details and examples of such agreements.

6.1.5. *Different circumstances where elements of process might be applied*

6.1.5.1. *When should an NRA intervene*

184. The objective of Article 28(2) is to reduce the overall instances of fraud or misuse to the benefit of end users by establishing an specific requirement for the Member States to ensure that the relevant authorities are able to require undertakings to block on a case-by-case basis access to number and services where this is justified by reasons of fraud or misuses and to require that, in such cases, providers withhold relevant interconnection or other service revenues. This requirement is also linked to the direct financial impact where instances occur, the lack of confidence in the integrity of numbers and in particular cross border services and the increased costs due to the cost of fraud or misuse incurred by operators.
185. One requirement is to reduce the impact of an instance of fraud or misuse that has occurred (and may be continuing) by blocking numbers. This will have the effect of preventing further calls, if the action is effective, and will limit the financial exposure to those parties that have been impacted. It will also prevent further revenue being generated by the people perpetrating the fraud or misuse on the particular numbers.
186. A second requirement is to require revenues associated with the fraud or misuse to be withheld. This can reduce the financial exposure to the end user and some or all operators of the chain. It may be possible to stop the revenues associated with these calls from being passed to the perpetrator of the fraud or misuse and hence discourage these incidents through this disruption.
187. It seems evident from NRA experiences of the levels of incidents that not having threshold below which an NRA will not normally intervene will result in NRAs and operators being swamped with cases of fraud or misuse. Therefore, recognising the limited resources in NRAs, other relevant authorities and operators, it is apparent that setting some threshold could optimise the use of the available resources. Such thresholds are for guidance and would not fetter the discretion of NRAs who wish to intervene in cases that fall outside these thresholds.
188. Since the harm is likely to impact end-users in the initiating NRA's jurisdiction, the primary responsibility for their protection must fall to this NRA, who must also take responsibility for the disruption of money flows as early as possible in the interconnection payment chain.
189. The value of the relevant originating traffic at will be dispersed as it is transits a number of different networks, depending on the traffic plan of the originating operator.
190. Given this dispersal, those NRAs through whose jurisdiction this traffic transits will assess the proportionality of requiring the withholding of revenue taking into consideration the value of traffic relevant to the jurisdiction.
191. The NRA in whose jurisdiction the relevant traffic terminates will have the primary objective of disrupting the money flow to the perpetrators of fraud or misuse.

6.1.5.2. *When is withholding of revenues likely to be required*

192. The withholding of revenues is likely to be required in circumstances where it is clear that fraud or misuse has been perpetrated. A necessary requirement for an intervention is that the victim of the fraud or misuse will have the impact of the incident reduced as a

result of the intervention or that the beneficiary of the fraud is likely to find that the intervention has had a negative impact. This may be through the disruption of the money flows or through an increased risk of detection.

6.1.5.3. When is number blocking likely to be required

193. Number blocking can involve the blocking of traffic from the A-number³⁵ and/or the blocking of traffic to the B-number³⁶.
194. A-number blocking is likely to be required on a short-term basis in the event of Artificial Inflation of Traffic, i.e. where the fraud or misuse is being generated from the A-number. This may, or may not be done with the knowledge of the legitimate end-user (i.e. the end-user to which the A-number has been allocated in accordance with the rules associated with number allocation in the relevant jurisdiction). The objective of A-number blocking is to stop the fraud or misuse where it is ongoing until such time as appropriate remedies can be put in place. Typically there could be selective blocking put on the end users line such as restrictions to international or premium rate services. Such blocking is useful in cases where the calling party perpetrates the fraud (e.g. in cases of ping calls). In cases where the legitimate end-user is unaware of the fraud being perpetrated, blocking of this A-number will have some impact. However this short-term impact must be balanced with the fact that such blocking, where appropriately implemented, will immediately stop the fraud or misuse.
195. B-number blocking is also likely to be required on a short-term basis, albeit for a longer time period than A-number blocking. The operator to whom the number has been allocated needs to conduct the blocking although this may not be effective if the calls are being terminated inappropriately on an alternative network through number high jacking or short stopping. B-number blocking may be possible for the Retail operator but operators block numbers in different technical manners. It appears that few are able to block individual B-numbers, relying instead on blocking numbers in groups of anywhere between 100 and 10000 numbers. Consequently B-number blocking may impact on those end-users that operate their numbers in good faith within the same number blocks. BEREC is of the view that it is possible that the effect on such end-users may in some circumstances be outweighed by the harm caused to those consumers who incur unauthorised excessive telephone charges as a result of falling victim to the fraud or misuse. Nonetheless, NRAs should be cognisant of this potential impact and act in a proportional manner when looking to block numbers. In particular it would be proportionate for the NRA in the originating country to block the whole range only if the NRA in the terminating country is not able or willing to intervene in the short term. This is particularly relevant in cases where the jurisdiction of the terminating NRA is outside the EU or EFTA member states.
196. In general, unless the B-numbers are terminating at an unknown and unauthorised destination, B-number blocking will be more effective if implemented by the terminating NRA, since this will ensure that traffic to these numbers is unable to reach the destination from any originating point. B-number blocking implemented by the

³⁵ The term "A-number" is used in this context to describe the telephone number associated with the calling party, or originating end-user.

³⁶ The term "B-number" is used in this context to describe the telephone number associated with the called party, or terminating end-user.

originating NRA will only stop traffic from that jurisdiction and therefore will be less effective. The latter should therefore only be used where necessary.

197. In many cases, however, it is clear that many of the numbers involved in cases of fraud or misuse are from blocks not legitimately allocated to end-users and in these cases, any disruption is entirely appropriate but care still needs to be exercised as such number ranges may be opened up by NRAs and operators for legitimate traffic in the future. It is therefore important that the relevant NRA is advised if interconnection to originating numbers from their numbering plans are blocked by the originating NRAs and operators.
198. Whether A- or B-number blocking is more appropriate will depend on the type of incident. For instance, in the case of PBX-hacking, where artificially high levels of traffic are being generated from a particular PBX – and therefore A number(s) to a number of different B-numbers – it is clear that A-number blocking will be more effective at disrupting the fraud or misuse and minimising the harm to the end-user. Likewise, blocking a short-stopped B-number will not have any effect; therefore blocking the A-number may be more appropriate.
199. On the other hand, an example would be where a large number of end users find their phones or PC devices making short calls to a few B-numbers. It is possible that the ability for a perpetrator to readily change the B-number being called is limited and hence blocking the B-number can be more effective.
200. The relevant NRA will need to take into account the level of disruption imposed on legitimate end-users prior to requiring an operator to block numbers.
201. Re-opening of numbers that are required to be blocked in the course of this process is a matter for the NRA who has jurisdiction over the numbering plan if appropriate in co-operation with the initiating NRA.

6.1.5.4. When is information gathering likely to be required

202. At the initiation of the process, certain information is required quickly to ensure the protection of end-users and timely disruption of money flows to the perpetrators.
203. The information required to be passed between NRAs includes the nature of the fraud or misuse, time and date of the start of the incident, the A and B numbers involved, and the transit and terminating carriers involved in the transmission of the call. This information should be developed by the initiating NRA and the next relevant NRA. The initiating NRA then has the responsibility to contact all other relevant NRAs in the chain as explained in section 6.
204. Information related to the A and B numbers are of particular interest as this will allow the relevant NRAs to identify more readily and hence disrupt the particular incident under scrutiny. Which number is more relevant (i.e. A or B number) will depend on the nature of the incident.

6.1.5.5. Sharing information with police or other law enforcement agencies

205. Some national processes (require that the incident be reported to the local police or other law enforcement agency prior to taking action. In these cases it may be necessary to share the information provided by operators and end users with these other agencies to assist them in their investigations.

6.1.5.6. Practical co-operation

206. NRAs requesting intervention or information from a second or further NRA or Relevant Authority should do so in written format. Given the time constraints associated with the implementation of this process, e-mail is an acceptable format.

Question 7: Are there other circumstances at which NRAs should consider intervention under Article 28(2)? Please give reasons for your response.

6.1.6. *Forum for reviewing process and thresholds*

207. BEREC believes that the process and related thresholds are appropriate for at least an introductory period, but also appreciates that review of these thresholds may be appropriate following a period of implementation.

6.1.7. *BEREC Office support*

208. The BEREC Office will manage the maintenance of NRA contact lists, so that the information needed is requested from the most appropriate expert within the NRA.

209. The BEREC Office will also track the number, type and location of incidents. This will facilitate the review of the thresholds, referred to in Section 5, and will also act as a knowledge base to assist NRAs in their investigations.

7. Protective measures that could be taken by NRAs, operators and end-users

7.1. Improving security

210. If the implementation of the BEREC process proposed and described in sections 5 and 6 of the report is designed to protect consumers and tackle fraud and abuses, in addition to the specific requirement provided for under Article 28(2), it should also be noted that it is clearly in the interests of operators to prevent fraud and misuse. Indeed the primary capability to prevent fraud and misuse lies with these operators and, in some cases, end users.

7.1.1. *Improving the protection of telecommunication systems*

211. In many cases of fraud or misuse, the origin of the case is the hacking of terminal equipment, and in particular Private Branch Exchanges (PBXs) equipment through their voicemail and maintenance ports. The access to the PBX is used by the hackers to make calls abroad, often terminating at premium rate numbers, causing businesses to run up important bills. Such incidents often occur outside of the business hours (during weekends or holidays).

212. It is the responsibility of end users (and notably businesses) to ensure that security settings which can be configured on the terminal equipment are in place.

213. As highlighted by ComReg in a recent information notice³⁷, businesses can avoid fraud or misuse such as PBX hacking, by taking simple steps, such as:

- Contact your telecommunications provider immediately and advise them of your concerns. Consider asking for calls to premium rate numbers and possibly international numbers to be barred;
- Contact your PBX supplier (if different from your telecommunications provider) and ensure that your PBX has the latest software updates to prevent unauthorised access and the latest security settings are enabled;
- Ensure that your PBX maintenance port has a strong password and not the default password;
- Ensure that your voicemail port has a strong password and not the default password;
- Restrict your voicemail service from making call forward calls if this feature is not used by your company.

214. Raising the businesses awareness regarding such security issues appears as one of the key action to tackle such fraud. NRAs, operators, as well as equipment manufacturers and suppliers have a role to play in informing businesses of the risks and solutions.

7.1.2. *Improving the detection of fraud and abuses*

215. The questionnaire on the scale/scope of the problem (see section 4.2) has shown that most of the interviewed operators have both automated and manual systems for detecting fraud or misuse on their network.

216. According to the majority of these operators, these systems enable them to detect almost all sorts of fraud or misuse identified in the questionnaire.

³⁷ "[Update on PBX Hacking](#)", Information notice, 16 December 2011, ComReg Document 11/100

217. As fraudulent traffic patterns might change frequently to avoid detection, operators should cooperate to share newly detected fraud patterns, adapt as quickly as possible all fraud detection systems and act consequently.

7.2. Moving to a self-policing role by operators for efficiency

218. The intervention of NRAs, based on the process described in section 5 and 6 of the report is expected to protect the consumers and tackle the fraudsters. Such intervention implies an important mobilisation in order for the NRAs to act in a timely manner, and if the cases are numerous, it may be rather time consuming to make all required verification.
219. In contrast, operators which are involved in such cases could efficiently directly deal with the issue, on the ground of contractual clauses.
220. As mentioned in section 4.2, the questionnaire on scale/scope of problem has shown that, if some international contracts include clauses allowing the operator to block the access to the service in case of artificially inflated traffic (AIT), or fraudulent traffic, almost none of the operators have claimed to be contractually able to withhold the associated revenues.
221. However, BEREC notes that a number of operators have expressed their willingness to insert such clauses in their contracts and support such evolution.
222. It can be expected that current BEREC's work on the subject of fraud and abuses, as well as the first decisions that may be adopted by NRAs in the next month on the ground of Article 28(2) will reinforce the incentive for operators to address the issue of fraud and abuses in their international interconnect contracts.
223. For instance, in the case where the originating operator is requested by the competent NRA to withhold the revenues, this measure may have an impact on the operator(s) which have transported the fraudulent traffic, since it is likely that all concerned NRAs will not necessarily be willing (or able) to intervene in all cases in order to impose the retention of revenues all along the chain.
224. By introducing relevant clauses, all operators may therefore be contractually entitled to take the initiative to withhold the revenue flow all along the chain in cases where the traffic is identified as fraudulent by the relevant authority and/or where, based on the evidence collected by the operator who initially take the decision to withhold the revenue flow, there is reasonable / strong suspicion there has been a fraud or misuse.
225. BEREC therefore encourages the operators to introduce such clauses in their international interconnect contracts and to address the issue in the relevant forums that exist at the European level (such as the GSMA fraud forum, FIINA, ETNO).

7.2.1. Cooperation with police or other law enforcement in member states to discourage incidents

226. In order to open the case, the NRA (or the "relevant authority") may consider useful that the operator and/ or the end user have previously reported the incident to the police or other law enforcement authorities.

227. More broadly, cooperation between NRAs and police or other law enforcement authorities³⁸ may be particularly useful to tackle fraud or misuse as the powers and expertise of NRA and such law enforcement authorities are very complementary in this respect.
228. According to their respective national law, such law enforcement authorities may not be able to disclose the information and documents collected to NRAs (or to the “relevant authorities”) in the course of criminal investigations. However, the police or other law enforcement authorities may inform the victim that the case can be reported to the NRA in parallel of the criminal investigations.

³⁸ And, more generally, all authorities involved in the prosecution of fraudulent practices.

Annex 1 – List of questions

Question 1: Are there other incentives or issues that will impact end users and/or operators that should be considered by BEREC? If this is the case, please propose and explain such incentives or solutions.

Question 2: Are there other issues related to the provision that are not discussed in this section that should be considered by BEREC? Please give details about your suggestions.

Question 3: Do the responses received and presented by BEREC represent an accurate reflection of the situation as experienced by operators and end users across Europe? Are there further aspects that should be considered by BEREC?

Question 4: Do you consider the proposed process to constitute a practical and effective method for NRAs to cooperate with each other in order to implement the requirements of Article 28(2)? Please explain your view with any suggestions you may have.

Question 5: Are these initial thresholds for retail operators and transit operators set at a realistic and practical level? Should other issues affecting whether NRAs initiate a case under this process be considered on a systematic, rather than ad hoc, basis? Please provide details on any proposals made.

Question 6: Are there other types of clauses found in typical commercial interconnection or other agreements that might influence the ability of operators to withhold interconnection revenues when required to do so by an NRA? Please provide details and examples of such agreements.

Question 7: Are there other circumstances at which NRAs should consider intervention under Article 28(2)? Please give reasons for your response.

Annex 2 – Questionnaire on scope/scale of problem

229. The following is an amalgamated outline of the responses received from NRAs to the questionnaire issued on the scope / scale of the problem of fraud or misuse in the context of Article 28(2).

Q1: Do you have automated systems for detecting fraud or misuse on your network?

230. Most of the interviewed operators have indicated that they use automated systems for detecting fraud or misuse. Those operators that stated that they do not use automated systems stated that they rarely had instances of fraud or misuse or that they considered that the fraud or misuse, when identified, required manual analysis.

Q2. Do you have manual processes for detecting fraud or misuse on your network?

231. All operators that responded stated that they employ manual processes in addition to automated processes where available.

Q3. On average, how often do you detect fraudulent calls or misuse on your network?

232. Operators that have fewer interconnections for international transit and/or termination state that they have fewer cases of fraudulent calls or misuse on their networks (for example, 4-5 cases per year) compared with those who have more interconnections for international transit and/or termination (The range of cases which are detected is from 1 incident per month to incidents detected daily).

Q4. What is the typical length of time before such fraud or misuse is detected on your network?

233. Some electronic communication operators indicated that the detection of fraud or misuse is done in real time, but the most respondents indicated that typical length of time to detect fraud or misuse on its network is 24 hours, with some exceptions where the typical length of time lasts several days. This demonstrates that operators have the ability to react in a timely manner.

Q5. Can you provide an estimate of the annual monetary value of fraudulent calls or misuse detected on your network?

234. Operators have indicated different levels of the value of fraudulent activities: from 6 000EUR to 19 000 000EUR. Spain noted that mobile network operators seem to suffer from 40 to 140 times more in the annual monetary value than fixed network operators. Some mobile operators tend to include subscription fraud in these figures.

Q6. Based on your experience, what do you estimate to be the overall monetary value of traffic resulting from fraud or misuse in your country?

235. Most respondents were unable to estimate the overall monetary value of traffic resulting from fraud or misuse. Some indicated 0.5-2% of overall revenue while others used indicative monetary value (200 000EUR - 2 000 000EUR).

- Q7. What percentage of detected fraud or misuse, at both retail and wholesale levels:
- originates and terminates within your own country?
 - originates and terminates within the EU?
 - originates or terminates beyond EU countries?

236. The percentage of fraud or misuse detected both at retail and wholesale levels differs among operators as well countries and even within countries itself (e.g. Slovakia). Most of respondents (Austria, Denmark, Latvia, Malta, Romania, Slovenia, Slovakia, Switzerland, Norway) indicated that the majority of (50% - 90%) detected fraud or misuse either originates and/or terminates outside EU countries.

- Q8. What sort of fraud or misuse are you able to detect? Examples are:
- PBX hacking
 - Artificial inflation of traffic (AIT) to a number within your country
 - AIT to a number in another EU country
 - AIT to a number in a country outside of the EU
 - Short stopping of international calls destined for another EU country.
 - Short stopping of international calls destined for a country outside of the EU
 - Calls to an unallocated telephone number in your country
 - Calls to an unallocated telephone number in another EU country
 - Calls to an unallocated telephone number in a country outside of the EU
 - Call back scams (also called "missed call scam" or "pinging")
 - SMS scams
 - other

237. Overall operators responded that they are able to detect almost all of these types of fraud or misuse (shown as example), with some exceptions.

238. Some operators have reported that they are also able to detect fraud affecting mostly business fraud (for example, subscription fraud, pre-paid fraud, shops fraud etc.)

- Q.9. What steps do you normally take when you have detected fraud or misuse (e.g. blocking access to a particular number, number range or country code; other action)?

239. Operators typically block access to a particular number in the first instance when they detect fraud or misuse.

- Q.10. Do you normally charge your customers who have been the victim of fraudulent activity, such as a PBX hack, the full retail charge for the fraudulent calls? If not the full retail charge, what do you charge?

240. Many responses explain that the retail customer is not generally charged for the fraudulent traffic. In other cases customers are fully or partly charged, but that depends of the details of the particular case.

- Q11. What standard of evidence do you expect?
- The retail customer to provide?
 - The wholesale customer to provide?

241. Most operators pointed that the standard of evidence required from either retail or wholesale customers is a reference to the relevant Call Data Records (CDRs) (which the operators will then investigate themselves) or a criminal complaint.

Q12. What patterns have you detected in fraud or misuse, for example are there common destination countries?

242. Overall the patterns are dynamic, but some main trends remain - calls to some international PRS/special services ranges generally to common destination countries (EU/Europe – Austria, Latvia, Bosnia, Bulgaria, France, Croatia, the UK, Liechtenstein, Poland, Moldavia, Slovenia, Italy, Spain etc., and beyond the EU- Cuba, Somali, Africa, Sierra Leone, Chile, Zimbabwe, Congo, Cook Islands, Bahrain, Pakistan etc.).

Q13. Do you have AIT (where AIT is artificially inflated traffic) clauses which enable you to withhold payments or block numbers:
 - in your national interconnect contracts?
 - in your international interconnect contracts?

243. The majority of operators explained that they have AIT clauses in national interconnection contracts which enable to withhold payments or block numbers.

244. Some operators reported to NRAs that they have a clause that allows them to block numbers in international interconnection contracts, but none reported that they are able to withhold payments in the international interconnection contracts.

Q.14. What, if any, contractual arrangements do you have within your international interconnection agreements for the withholding of payments or blocking of numbers (for any reason)?

245. The majority of respondents reported that they do not have provisions within their international interconnection agreements for the withholding of payments or blocking of numbers (for any reason).

Q.15. How many network operators do you interconnect with for international transit and/or termination?

246. Some operators have indicated they interconnect with one while others interconnect with up to 500 other operators for international transit and/or termination.

Q.16. If more than one, are you able to track the precise routing of an individual international call originating on, or transiting across, your network?

247. Most of operators responded that they are able to track the precise routing of an individual international call originating on, or transiting across, their network.

Q.17. Do you share information/intelligence on fraud or misuse with any other network operators in your country or abroad?

248. Responses confirm that operators usually share information/intelligence on fraud or misuse with other network operators in their country or abroad.

249. Some operators stated that they inform other operators (countrywide, mother branch companies) and some operators indicated that they share information with GSMA, ETNO, FIINA (Forum of International Irregular Network Access) and CFCA (Communications Fraud Control Association).

Q.18. Do you share information/intelligence on fraud or misuse with any enforcement agencies in your country? If so, which ones and what is the nature of the cooperation?

250. Some operators indicated that they share information on fraud or misuse with enforcement agencies in their countries. Typically they share information with the NRA or police to support cases of investigations in individual cases.

251. Those who replied no, remarked that such information is only shared if legally permitted and necessary, as in many cases legal prosecution of fraud or misuse is very time consuming and often unsuccessful. Thus the operator rather focuses its activities on the detection of fraud or misuse and on trying to make such activities unattractive for those trying to commit fraud or misuse.