Body of European Regulators for Electronic Communications

BEREC

BoR (13) 36

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

Consultation Response Analysis

7 March 2013

Contents

Introduction

1. In this document BEREC provides its comments to submissions received in respect of document reference: "BoR (12) 85 Article 28(2) Universal Service Directive: A harmonised BEREC cooperation process – consultation paper[1]" ["the Consultation"].
2. This document should be read in conjunction with the Consultation, the responses to the Consultation as published here and the final document "BoR (13) 37 Article 28(2) Universal Service Directive: a harmonised BEREC cooperation process – BEREC Guidance paper" ["BEREC Guidance Paper"].
3. Comments relating to the consultation were received from BT, Cable & Wireless Worldwide (CWW), ETNO, Eircom, Federation of Communication Services (FCS), GSMA, Telecom Austria Group (TAG), Telecom Italia, the Telecommunications UK Fraud Forum (TUFF), Verizon, Vodafone and a respondent that wishes its response to remain confidential (a Respondent). Reference is made to the specific aspects mentioned in the responses received.
4. Respondents generally welcomed the action by BEREC in respect of addressing cross border cooperation relating to fraud and misuse pursuant to Article 28(2) of the Universal Service Directive ("Article 28(2) USD") stating that the BEREC draft process is in its view a very positive starting point.
5. A number of points were raised by respondents covering points such as:
    a. Views on the need for and likely effectiveness of the process
    b. Consideration as to the process being more prescriptive around national implementation
    c. The definition of fraud and misuse
    d. The use of thresholds
    e. The impact the process will have on stakeholder incentives for appropriate security
    f. The approach to cases going beyond EU borders
    g. The need for timely intervention and the problem with short payment timescales in contracts
    h. BEREC's role in respect of information dissemination
6. Some respondents expressed views about the challenges that will be faced by stakeholders with an overall recognition that there is a need for an industry approach to combating fraud or misuse although there are a number of difficulties that will be faced.
7. A number of general comments have been grouped with related points and addressed in the sections below.
8. Although no responses were received from consumers associations or other stakeholders active in consumer protection at national or EU level, BEREC notes that due consideration is given in the BEREC process to the protection of end-users[2]

[1] http://berec.europa.eu/eng/document_register/subject_matter/berec/public_consultations/979-draft-berec-report-on-article-282-universal-service-directivea-harmonised-berec-cooperation-process-consultation-paper

[2] The definition of end-user for the purposes of Article 28(2) would primarily follow the definition under Article 2 of Directive 2002/21/EC (Framework Directive): "end-user means a user not providing public communications networks or publicly available electronic communications services".

interests and rights in cases of fraud and misuse in line with the objectives of the Directive on Universal Service and end-users rights.

Consideration of points raised by respondents

Standardisation and consistent application

9. A number of respondents considered that for the process to be as practical and effective as possible, it required further development to ensure it was delivered in a standardised and consistent manner across Member States. Some respondents were concerned that differences in national regulatory and judicial frameworks, which could result in NRAs reaching contrary positions on a case of fraud or misuse, would put the effectiveness of the process at risk.
10. CWW noted that the process was described in the consultation paper as non-binding and based on NRAs' discretionary powers. CWW raised concerns about the case-by-case nature of regulatory proceedings currently and argued that NRAs should follow standardised processes for national and particularly cross-border cases, with the use of discretion minimised. CWW also considered that some NRAs would need to change their approach to react to relevant cases with sufficient priority, otherwise there would be confusion over how and when national procedures would result in intervention.
11. Verizon considered that consistent application across Member States should be the goal of the process, rather than merely fostering appropriate communication between NRAs, which should already exist. Telecom Italia and GSMA considered that the process could be effective if all NRAs followed the same rules and criteria for intervention, ensuring that if one NRA issued a direction for operators to withhold payments, all NRAs in relevant countries to the case would also direct the withholding of payments. Without consistent application, CWW questioned what would happen in cases where NRAs did not proceed as expected, particularly with regard to transit providers whose NRA had not directed them to withhold revenue. GSMA considered that a consistently applied process was necessary to protect operators from financial loss and limit damage to commercial relationships.
12. BEREC agrees that benefits may be derived from the standardised and consistent application of a process. The process put forward for consultation is intended to deliver a commonly understood procedure for coordination and cooperation between relevant authorities in cases of fraud and misuse focussing on end-users in accordance with article 28 (2) USD[3]. It forms a set of guidelines to be used by parties involved in cases of fraud or misuse so that information can be shared in an effective manner and appropriate options for intervention considered and taken where appropriate.
13. However, as mentioned by some respondents, differences in national regulatory and judicial frameworks do exist. As a consequence, different approaches to action and intervention may result from the relevant authorities in different countries. Nevertheless, through BEREC's development of a common process and its

[3] See paragraph 39 of the Guidance Paper.

subsequent implementation and refinement, it is expected that a certain level of standardisation and consistency will result, as well as collective NRA participation in the process.

Governance and participant roles

14. Clarity on the governance of the process was also seen by respondents as an important aspect for its success. CWW stated that from an operator's point of view, national judicial and regulatory rules created a duality of roles and positions, with potential confusion over the governance of any resulting proceedings. CWW was unclear as to how the process would proceed in situations where judicial proceedings and NRA investigations came to different conclusions on a case.
15. BEREC recognises stakeholders' uncertainty over governance of the process. The position is that the process will provide guidelines and a framework for coordination and information sharing between NRAs in cases of fraud and misuse. The level of control assigned to relevant national authorities in responding to cases of fraud and misuse is a matter of national implementation, and this will dictate how cases proceed where national judicial proceedings and NRA investigations reach different conclusions on a case.
16. CWW also felt that the roles assigned to different participants in the process needed to be agreed. In particular, the consultation paper implied that responsibility for investigating a case would move from operators to the NRA. CWW asked BEREC to confirm that this role had been commonly agreed by each NRA and to clarify what the appeal process would be if an operator disagreed with the outcome of an NRA's investigation.
17. At this stage BEREC is providing the framework for coordination. BEREC is planning an implementation exercise for the process and intends to work with stakeholders to agree and refine participants' roles. Implementation and participation will be an ongoing process and roles should become more clearly defined with experience. For the avoidance of doubt, the process is not intended to replace operators' investigation of fraud or misuse. Rather, it is intended to supplement the work operators undertake in investigating cases of fraud and misuse.

Legal framework

18. CWW asked about the legal basis for the process. In particular, CWW considered that each action taken by NRAs in relation to the process needed reference to a legally binding framework in order to provide participants with legal certainty. Specifically, CWW requested clarification from BEREC on whether NRAs in transit countries were empowered by Article 28(2) USD to intervene.
19. One respondent called for protection for operators from any legal consequences arising from the reporting of cases of fraud/misuse. This includes protecting providers from liability for any direct or indirect damages that any third party may suffer from the reporting of a wrong number. The respondent also suggested that a terminating or transit provider that repudiates a notified number should be liable for further losses due to fraud/misuse that occurs after the refutation occurred.
20. BEREC considers that the legitimate legal basis for NRA cooperation as envisaged by these guidelines is Article 28(2) USD. Within the EU regulatory framework, this Directive, and in particular its chapter IV, aims primarily to establish and protect the interests and rights of end-users and the corresponding obligations of undertakings

providing publicly available electronic communications networks and services. Furthermore, Article 28(2) USD appears to establish the general obligation for Member States to enable national authorities to establish specific requirements on undertakings providing public communications networks and/or publicly available electronic communications services. This explains BEREC's intention to focus on end-users interests and rights and the resulting obligations for undertakings under Article 28(2) USD. BEREC would also note that it considers that fraud or misuse impacting an undertaking may also be considered to have an end user impact as it will potentially impact on costs for services and hence prices to end users. The purpose of the Guidelines therefore also encompasses the protection of undertakings affected by fraud or misuse cases, as expressly stated in paragraph 20 thereof. The foregoing is without prejudice to the intervention by independent NRAs to tackle fraud and misuse cases in the context of other provisions of the EU Framework[4]

21. BEREC understands respondents' desire for a clear legal framework to support the process. However, the process is essentially a set of guidelines to assist NRAs (and other relevant authorities) in the implementation of the requirements in Article 28(2) USD for cross-border cases of fraud and misuse in the most effective manner. The guidelines are not legally binding and can not be used to provide legal certainty for participants. Resolution of the relationship between regulatory and legal frameworks will need to be considered on a national basis in order to resolve the specific questions raised by respondents.

Definition of fraud or misuse

22. CWW, FCS and Orange considered that a common description of fraud and misuse, as binding concepts, would be expected to harmonise the application of the concept and the adoption of measures, thus harmonising national actions, making easier the application of contractual provisions and improving the end-to-end effectiveness of interventions.
23. As indicated in the consultation, BEREC notes that the notion of fraud or misuse is not defined in the USD and therefore it is the competence of the Member States to apply these requirements in accordance with national law transposing EU law. BEREC notes that in accordance with Article 40 USD, the Directive is addressed to the Member States. While respecting this national competence, one of the purposes of the BEREC harmonised process is precisely to provide a common framework of interpretation through examples of potential fraud or misuse across the EU to facilitate the consistent application of article 28 (2) USD in cross-border situations.

The common process as a supplement to Operators' own procedures

24. A number of operators stated that the common process needed to operate in parallel with (and not replace) operators' own procedures for protecting their customers.
25. Telecom Italia and GSMA requested confirmation that operators would have the ability to block access to numbers and payments independent of any NRA direction to do so, plus clarification of how operator control over number blocking would work alongside the process. GSMA argued that it was essential mobile providers retained

[4] E.g. pursuant to articles 20 and 21 of the Framework Directive or in the context of article 5 of the Access directive.

the ability to block or unblock access to numbers, depending on their independent commercial assessment of the associated risk of fraud. It also stressed the importance of operators being able to intervene swiftly in cases of fraud to protect their customers, as opposed to unnecessary delaying action while an NRA or other authority builds evidence for a case.

26. BT stated that communication providers should take reasonable measures before blocking calls to a number and should gain as much information as is reasonably possible about the situation prior to blocking. Such measures could include checking whether the number is to a known location where fraudulent activity has been previously identified.
27. BEREC agrees that the common process should run in parallel with operators' own procedures for protecting their customers from fraud or misuse, as furthering the interests of consumers is the paramount consideration. The independent action that operators may take depends on national regulation.
28. With regard to the suspension of interconnection or access to services, this measure is not envisaged as an approach that will be employed by operators as a matter of course, particularly as a specific requirement under Article 28(1) USD is that all numbers should be open to end users. It is however possible that in the event of fraud or misuse cases some NRAs at implementation level may have agreed processes with undertakings around the blocking of numbers for termination or access of calls in specific circumstances. This is not an area that is specifically addressed by the BEREC process but BEREC would note that undertakings often have to deal with these issues in real time whereas the relevant authority may not be aware of the problem for some time, therefore a national process for such rapid intervention in this area may be considered by the NRA to be appropriate although such action would need to be consistent with Article 28(1) USD.
29. BEREC notes that reviewing the specific details of those fraud or misuse cases that are investigated is essential and therefore agrees that it is necessary to have as much information as possible in relation to such cases.

The process needs to be simple to operate and well-maintained

30. Some respondents noted that wide stakeholder engagement was necessary for the process to have value and therefore its operation must be kept simple to ensure this. In particular, the arrangements for reporting suspicious numbers needed to be made as attractive as possible for operators, as they would be the key providers of the necessary data. Also, there was a need for NRAs to commit to the process, including educating participants in the details of its operation (e.g. training participants, ensuring consistency and assessing effectiveness) and ensuring data is kept up-to-date. A respondent stressed that the necessary resource and funding required for those tasks should not be underestimated.
31. BEREC has sought to develop a process that will be workable across Member States (and ideally beyond) that balances effectiveness with an appropriate level of intervention and uses measures that are quick to initiate, simple to operate and can progress to a satisfactory outcome. Achieving these aims is important for the process to be successful and BEREC agrees with respondents that each aspect of the process needs to be as straightforward as possible for the relevant parties to encourage stakeholder engagement.

32. It is also essential that the process is well-maintained and participants are made aware of its function and their roles. This requires input from all participants, although it is recognised that NRAs will have a particular role in raising awareness of the process and educating national stakeholders in its operation. BEREC also has a role in raising awareness amongst participants and is planning an implementation exercise including a workshop to promote stakeholder understanding and encourage engagement.
33. The process is intended to assist NRAs in the implementation of the requirements in Article 28(2) USD. BEREC considers that the resource needed to manage the process should not be additional to the resource already required for relevant authorities to take action as required by the USD.

Impact on Operators

34. Some respondents raised concerns about the impact of the process on operators. TAG and GSMA argued that the proposed process would be harmful for the telecommunications industry as it would disrupt relationships between operators and could undermine commercial confidence in the interconnection payment chain.
35. CWW considered that the majority of fraud cases would involve countries where the common process is not adopted. As a result, CWW was concerned about the financial impact on operators where the fraudulent call is carried through the EU and terminates outside Europe. This would put transit providers at financial risk and, CWW argued, NRAs should shape their intervention in a way that limits the financial impact on these operators, particularly as the transit provider is not involved in the abuse/fraudulent activity.
36. BEREC acknowledges some respondents concern over the proposed intervention of NRAs in operators' ability to make payments in accordance with contractual agreements for the handling of call traffic relating to cases of suspected fraud or misuse. BEREC has kept the impact of regulatory intervention in mind when devising the process and has sought to minimise this through the development of guidelines on the implementation of Article 28(2) USD. While some respondents have raised concerns that differences in national regulatory and judicial rules will lead to inconsistent application and will expose operators in some countries, particularly those providing transit services, BEREC considers that the flexibility provided by the process would allow NRAs to shape their action in a way that recognises the impact on the operators involved within their jurisdiction and ensure an appropriate level of intervention.
37. Some respondents commented that the process would have an impact on operators' resources. For instance, GSMA noted that while the proposed process would be regulatory driven, most of the work related to identifying transit providers would be undertaken by operators.
38. BEREC does not consider that the process would necessarily increase the burden on operators' resources to any great extent, for they would already be involved in operator-initiated investigation of cases of fraud and misuse.

Blocking access to numbers or services as a last resource measure

39. ETNO stressed that number blocking should be considered as a measure of last resort, since it has technical limitations and blocking can generate further issues when blocked numbers are assigned to a different undertaking or when the number

is called by end users belonging to other undertakings. Number blocking should remain a possible measure in some cases as it can be a quick and effective method to protect customer from further harm. If there is sufficient proof of fraudulent traffic on some numbers, there is limited risk that customer will request access to these numbers to be reinstated.

40. BEREC agrees with ETNO and notes that the document subject to consultation underlines that "NRAs should be cognisant of this potential impact and act in a proportional manner when looking to block numbers" [in accordance to the requirements established under Article 28(2) USD] (paragraph 196 thereof).
41. TUFF further remarks that "When an NRA is considering [issuing] a directive to block service it must consider the technical feasibility of doing so by the network operator as not all services may be able to be blocked without adverse impact on other services/customers."
42. ETNO notes that "blocking access can only be done if technically feasible. On the other side the accessibility of numbers throughout Europe should also remain in balance with the risk of fraud and with the real demand for this accessibility".
43. BEREC agrees with these remarks noting that there are scenarios where number blocking is impractical, such as blocking origination numbers in a Wangiri incident (short calls to many numbers to stimulate ring back) and generally termination numbers in international revenue share fraud or misuse such as short stopping of numbers because there are so many numbers that can be used. The Consultation underlines that NRAs should take into account the potential impact of such measures and act in a proportionate manner when looking to block numbers. Regarding the issues linked to the cross-border accessibility of number, please refer to the BEREC Report on the Current Accessibility of Numbering Resources Pursuant to Article 28(1) USD.
44. Eircom argued that action from an operator to block access and withhold payments should be mandatory following a direction from the relevant NRA to do so, as this was an integral part of the process.
45. BEREC confirms that, under national regulation, operators should be required to follow directions from relevant authorities to block access to numbers and withhold payments.

Retrospective withholding of payments

46. CWW noted that the timing of any action taken in respect of requiring the withholding of revenues is important. CWW specifically asked "Where payments have been released in relation to the actual suspect calls, will the NRA have the authority to stop subsequent payments from future months for the equivalent value associated with a case they are dealing with?"
47. BT suggests that the Guidelines should allow for retrospective retentions to be made to incentivise the appropriate level of due diligence in Communication Providers' business relationships. Article 28(2) USD should take precedence over contractual obligations relating to payment for fraudulent traffic, even traffic carried in "good faith".
48. BT considers that "Where money has been paid out as a result of a service which has subsequently come under investigation, recovery should be possible retrospectively, even after an initial payment has been made downstream to encourage due diligence for transit carriers. […] For clarification if fraud or misuse is

identified as per the BEREC guidelines, out-payments should be recoverable or off-set against future payments. This is necessary to allow for the time taken to identify the fraud, the collation of Call Data Record's and other relevant evidence, and the routing information and values relating to minutes and revenue to be collected."

49. BT also stated that Communications Providers who have passed on revenue in good faith, or are in the process of making payment, should not be adversely affected by the process.
50. BEREC does not consider that Article 28(2) USD expressly covers the possibility of retrospective retentions and therefore the Guidelines do not expressly refer to this possibility in the context of the enforcement of article 28 (2) USD. BEREC considers that the approach to this issue will be addressed by the NRA in consideration of national legislation. BEREC agrees with the statement that Article 28(2) USD takes precedence over contractual obligations. The foregoing is without prejudice to the possible agreement between the undertakings covering a retrospective retention of amounts corresponding to fraudulent traffic. BEREC would encourage undertakings to ensure contract changes accommodate repayments of relevant charges where the calls are identified to be fraud or misuse. This contractual approach will allow more time for undertakings to investigate the circumstances of a claim.

Improving security and the protection of telecommunication systems

51. Verizon considered that, as an observation to paragraph 27 of the Consultation which states: "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", there is a natural read-across in the Article 28(2) USD provisions to the provisions of Article 13(a) of Framework Directive ("FD"). Article 13 specifies that undertakings should take appropriate technical and organisational measures to manage risks posed to security and appropriate steps to guarantee the integrity of networks. Verizon suggested that this should act as a very strong incentive on all undertakings to put in place adequate security measures to rapidly detect and mitigate the impact of fraudulent or potentially fraudulent traffic. Where the same originating operator is subject to an Article 28(2) USD investigation on more than one occasion, the responsible NRA should consider using its powers under Art 13 of the FD to order a full audit of the systems and processes in place at the operator. This type of scenario would be exactly when these powers under the FD should be used.
52. BEREC notes that the scope of the present exercise is limited to Article 28(2) USD and in such context wouldn't exclude the application of Article 13 of the Framework Directive in situations of fraud or misuse but does not consider that it is necessarily relevant in all situations. BEREC does not consider that Article 13 of the Framework Directive dealing with security and integrity of networks and services expressly endorses the interpretation proposed by Verizon with regard to fully auditing undertakings subject to an investigation pursuant to Article 28 (2) USD. BEREC also notes that Member States may provide the enforcement of each of these provisions to different national authorities.
53. Telecom Italia adds that, as the fraudulent / misuse phenomena evolve, it is not sufficient to limit enforcement actions to block / suspension of services and / or payments, but in addition it is desirable to strengthen the security of services in order to protect customers and operators, or adopt hardware / software techniques of protection for certain services (e.g. in Italy the introduction of PIN numbers has been

used to reach VAS numbers). It should be noted that in some cases the fraud takes place during the process of access to the service and therefore, in these cases, the block of payments is an ineffective intervention.

54. GSMA and Orange suggest that there is little incentive for an undertaking to increase security for retail traffic originated on their network if they have a route through which they can block onward payment to their carrier. In fact, if undertakings providing services to end users are able to not pay for traffic that is fraudulently generated, they may decide to reduce their investment in front end and detective controls as these are no longer required in order to manage the financial risk of fraud. The existence of a payment withholding process for fraudulent traffic which reduces the risk to retail undertakings may give them an incentive to offer greater access to services to end users. In the absence of such a process, high-value and/or high-risk services might only have been available to customers after a proven payment history or following receipt of a deposit.
55. Similarly, CWW submits the possibility that the knowledge that there will be no need for an affected End-User(s) to pay in the event of fraud or misuse will reduce the incentives to maintain appropriate and effective technical safeguards to protect the end users infrastructure from fraud and hacking.
56. BT proposes that at a retail level, minimum requirements should be defined for Communications Providers to put in place efficient systems and processes to detect and handle fraud and ensure sufficient end-user protection. Similarly, BT proposes to define minimum expectations / security requirements to ensure that responsibility for debt is not deflected by the end customer as the result of article 28 (2) USD. Finally, in BT's view guidance and awareness of the minimum security requirements for end users would help to reduce volume of incidents and the cost of managing disputes.
57. With regard to incentives on increasing the security of the networks and services, BEREC agrees that good security by undertakings and end users is very important. In this context, operators and carriers should take into consideration the fact that the BEREC process entails cooperation between NRAs but does not necessarily lead to an NRA intervention. In these conditions, the undertakings should consider the incentives on maintaining the appropriate security safeguards. The details on the implementation of security measures at the undertakings or end users level go beyond the scope of the Guidelines for the BEREC process. In any event, BEREC would agree that raising awareness of the issues with end users and undertakings and encouraging appropriate vigilance is desirable.
58. GSMA notes the retail communications industry is also moving progressively towards flat-rate tariffs for international call services, commonly allowing customers to make unlimited calls to various international destinations for a single monthly price. In contrast, international wholesale interconnect voice traffic is metered on a per-minute basis. In this environment, the risk to consumers for international fraudulent calls is reduced, but the risk to undertakings from fraudulent abuse of such packages is increased.
59. BEREC notes that undertakings may limit their risk exposure by contractually excluding high-risk destinations from their flat rate packages and notes that numbers an undertaking chooses not to include in a flat rate scheme may be charged outside such a flat rate scheme. Alternatively, undertakings availing of broad flat rate charges for international calls should consider whether their fraud detection processes are adequate for such a scenario.

60. BT remarked that “Minimum expectations/security requirements for end users should be defined to ensure that responsibility for debt is not deflected by the end customer, as a result of Article 28(2) USD, as per the guidance provided in Section 7.1.1 of the BEREC consultation document”.
61. ETNO considers that “the option to reimburse an end-user who was subject to fraud should be carefully considered before application. It should not be considered as a general principle nor should it be communicated as such. Such principle could have negative impact in our fight against fraud and is not justified as a general measure”.
62. BEREC underlines that is necessary to raise end users awareness regarding the need to improve their security, and to maintain the incentives for end users to do so and would encourage retail undertakings to appropriately inform their customers of potential risks. It is clear that the relevant authority will take into consideration a number of factors when deciding whether to take action in support of an end user or undertaking and consequently it would be imprudent of end users or undertakings to assume that such an intervention was inevitable.

Examples of Misuse or fraud for the purposes of Article 28 (2)

63. A number of scenarios were suggested by respondents as being appropriate to be considered as fraud and misuse.
64. BT suggests that the process could also be used to address the many types of misuse and ‘nuisance’ (e.g. abandoned and unsolicited sales and marketing calls and SMS texts) where what is often a scattergun approach is used which ends up causing harm, annoyance and anxiety to end users.
65. BEREC considers that the process can be used to the extent that there is fraud or misuse but we would note that such incidents may fall into the realm of data privacy (Article 13 of Directive 2002/58/EC (ePrivacy Directive) and be handled by other parties and other processes.
66. BT also indicated that it had “identified instances of abuse of the Divert and Call Forwarding Services in order to perpetrate fraud. Specifically the use of Divert and Call Forwarding Services to result in a calling pattern which is disproportionate to the overall duration and/or extent of calls which would be expected from good faith usage.”
67. The Consultation provides an indicative list – which is not comprehensive – of practices that generally can be regarded as fraud and/or misuse. It is possible that a scenario as identified by BT would be considered to be AIT, depending upon the actual circumstances, as therefore covered by the current examples of fraud and misuse.
68. BEREC considers that the examples given in the consultation are consistent with the suggestions from respondents except where noted in this document although some of the proposals from respondents may be better described as indicative of fraud and misuse as an NRA may consider that no fraud or misuse has occurred. For example, a breach of the European CLI rules such as masking the CLI, or the use of a number that does not identify either the calling line or mobile device, (except when the number is provided as an additional calling party number alongside a number that does identify the calling line or mobile device) would be quite likely in some circumstances to be associated with fraud or misuse. BEREC notes that the EU regulatory framework contains specific provisions regarding calling line identification

(Article 29 USD on additional facilities which include calling line identification) and unsolicited communications (Article 13 of Directive 2002/58/EC (ePrivacy Directive).

69. Similarly, a respondent suggested that the use of a number by a party to whom the number was rightly allocated, to generate calls to a Premium Rate Service or to an international number in proven contradiction with the terms and conditions of the offering of the Retail Operator the party purchased its service from would represent a fraud or misuse.
70. BEREC would not agree that the description given would necessarily constitute fraud or misuse as the definition is too wide however it is possible that such an incident would constitute AIT which is currently in the proposed list.
71. In BT's view, the focus of this consultation appears to be aimed specifically at the Artificial Inflation of Traffic (AIT) to Premium Rate Services and International Revenue Share Fraud. Subscription Fraud and PBX/Virtual PBX Fraud, for the purposes of Call Selling, should also be covered, especially in relation to identifying the perpetrators who have profited from these types of fraudulent activity.
72. BEREC considers that a significant amount of the fraud or misuse identified recently results in AIT but would not exclude other potential types of fraud or misuse from the application of these guidelines.
73. Telecom Italia is of the opinion that a basic definition of different fraud cases would be useful. In Italy they have experienced a strong benefit in the combating of these phenomena using a precise list of definitions, which are written into their interoperator contracts signed by all the main undertakings under the auspices of AGCOM in 2010. Specifically Telecom Italia quoted the" Interoperator Protocol" which provides a non-exhaustive list of cases that have been officially considered fraud in Italy, and proposes a list of phenomena that fall within the general definition of fraud. Telecom Italia also refers to the concept of "abnormal traffic" that can take infinite forms, not all being predictable.
74. BEREC agrees that a list of the types of fraud or misuse which would be covered by this process is helpful and this is addressed in this response to consultation. It should be noted though that the list of examples is not exhaustive as fraud and misuse develops with time as new opportunities or weaknesses are uncovered.
75. GSMA consider that the consultation paper does not mention roaming of mobile subscriptions and there is ambiguity about the responsibilities of operators and the definition of fraud origin with regard to roaming SIMs. Roaming needs to be fully considered from the perspectives of incentives, process, and thresholds for intervention.
76. TAG stated that a shortcoming of the process is "the lack of taking roaming of mobile subscription into consideration". BEREC understands this to be referring to the use or misuse of mobiles when roaming such as for AIT to premium rate numbers in the country in which they are roaming.
77. FCS also considers that roaming fraud should be dealt with as part of the Process. FCS notes that the nature of roaming fraud means that process should aim to alleviate any delays in detection. This is further commented upon by Eircom. They state that this is a particular area where fraudsters can expose weaknesses in the existing cross-border processes that are in place and the potential for this type of fraud is more significant for operators than other frauds. Due to reporting delays operators may not become aware of roaming fraud for a number of days rather, than a number of hours if the customers were not roaming. Furthermore the BEREC

Process needs to provide clarity on which NRA and operator will take the lead in tackling incidences of fraud against roaming customers.

78. BEREC considers that the scenario where a roaming mobile is used to generate artificially inflated traffic to a destination number is potentially a form of fraud or misuse and would anticipate the process can be applied when the issue is brought to the attention of an NRA, probably in the country in which the mobile is roaming.
79. Eircom also addresses the specific case of roaming services stating that there is a particular exposure when fraudsters target customers that are roaming. Due to reporting delays operators may not become aware of this particular fraud for a number of days rather than a number of hours if the customers were not roaming. Furthermore the Process needs to provide clarity on which NRA and operator will take the lead in tackling incidences of fraud against roaming customers. Will the lead be taken by NRA in the home country of the customer's network or the NRA in the country where the roaming occurs?
80. In response to these comments regarding roaming and as pointed out in the description of the situations that could qualify as fraud or misuse, BEREC reiterates that for the purpose of the BEREC process the concept of fraud and misuse is open in order to respect the specific transposition at the national level of Article 28(2) USD and the document lists on a non-exhaustive basis situations that are commonly qualified as fraud and misuse and which include short-stopping and artificial inflation of traffic using roaming services. As to Telecom Italia's reference to "abnormal traffic" and since the conditions under which such "abnormal traffic" may take place could be diverse, it would not be appropriate to define specific circumstances. BEREC notes, however, that abnormal traffic may depend on the duration of the calls, the reiteration in the calls to the same number, etc. In response to BT, BEREC notes that providing false information in the subscription or provision of electronic services and identity thefts leading to AIT are also included as examples of forms of fraud or misuse (see paragraph 49 thereof). The specific case of roaming frauds may result in the fraud or misuse being identified in the jurisdiction where the calls are made or the jurisdiction where the retail contract exists. BEREC considers that either jurisdiction may be asked to initiate the case and the process is not prescriptive in that regard but there will need to be coordination between the relevant NRAs to agree the appropriate handling of the incident.
81. In the opinion of Eircom, the consultation document suggests that Premium Rate Numbers (PRNs) represent the largest fraud risk. In Eircom's experience PRNs fraud is a significant issue, however fraud utilising geographic numbers that are 'short-stopped' is of greater concern. Eircom has direct experience of fraudsters targeting geographic numbers which are hijacked or short-stopped. The proposed Process should ensure that this type of fraud can be dealt with effectively through number blocking and the withholding of payments.
82. BEREC would agree with Eircom's assessment that short stopping is currently a significant issue and considers that the process should address this form of fraud and misuse.
83. GSMA and Orange considered that the document focuses exclusively on a legitimate end user and this concept needs to be developed to also consider a fraudulent end user. GSMA notes that "…..in many cases of organised fraud and misuse, a dishonest end user acquires service fraudulently with the intention of abusing operator services in order to artificially inflate traffic and dishonestly generate

revenue. […] The proposed BEREC process should disrupt end users who fraudulently generate calls on operator networks while also protecting legitimate end users, who may suffer from the consequences of fraud."

84. BEREC agrees that there are forms of fraud or misuse where the end user is an active participant and considers that such cases may also be subject to the application of Article 28(2) USD, but notes that other provisions of the EU Framework may also have to be considered. BEREC would however observe that where the fraud or misuse is an exploitation of poor security in operator processes or services an NRA may consider that an operator should have a greater awareness of the potential for fraud or misuse than a typical end user. This may be a factor which an NRA takes into consideration when deciding whether it is appropriate to intervene.
85. GSMA and TAG noted that "Member State NRAs should look at the retail businesses and service providers linked to recurring fraud events in their countries and work with them to determine the cause of recurring frauds. The process proposed by BEREC could be selectively applied in such scenarios, in combination with other investigative support."
86. BEREC agrees with this remark and considers that the fact that a retail business, or a service providers, is linked to recurring fraud, may be taken into account by the NRA for the purpose of deciding whether to intervene or not.

Timescales for intervention

87. Verizon notes that most if not all carriers / operators will work to strict tightly controlled payment schedules for invoicing and paying one another. If action is to be taken which will have an impact on the processing of payments and/or the flow of revenue between operators, it must take account of these schedules, and the associated approval processes which typically precede actual payment. Verizon has significant concerns, based on recent experience, that NRAs may not take full and proper account of the need to act swiftly and in accordance with the operational needs of the providers involved. Indeed any process envisaged may be simply too slow and / or complex to be effective, given the diverse number and type of stakeholders that may be involved in any one case. Verizon considers that it is essential that some form of SLA is developed and agreed by NRAs that all stakeholders can buy into, or at least use as a means to fully understand their rights and obligations from the start. They consider that this will give providers confidence that NRAs are accountable for, and transparent in, their actions. It should also help to reduce uncertainty about NRAs acting in a coordinated or efficient manner.
88. In response to the questions raised on the effectiveness of the BEREC process, BEREC reiterates the importance of a swift intervention by NRAs. BEREC does not consider it appropriate to require SLAs at a national level but clearly all parties, NRAs, undertakings and end users need to act in a timely manner for this process to be effective.
89. Orange notes that BEREC proposes that NRAs deal with other NRAs as a first point of contact in Member States, even where some or all the responsibilities associated with Article 28(2) USD have been given to another body in a particular Member State. Orange supports the proposal in the context of cross-border fraud or misuse cases but suggests there is a requirement for BEREC to work with providers and NRAs to determine relevant service levels. Orange also notes that in some cases service providers may require payments within 7 days.

90. In addition, BT warns that careful consideration should be given to the time required to identify fraud and misuse, identify Call Data Record volumes and minutes, determine the flow of traffic and revenues, particularly bearing in mind the fact that many International Premium Rate Number Providers offer very quick pay-out terms, often within 7 days.
91. ETNO states that a speedy decision regarding blocking numbers or withholding revenues is essential, due to the timing of payments and the type of service provided.
92. Telecom Italia suggests that the cooperation process between BEREC and NRAs should also establish direct and agile channels dedicated to fraud/misuse in NRAs, in order to facilitate and speed up their mutual communication in the event of cross border fraud and misuse.
93. BEREC agrees that the process needs to be expeditious to accommodate contracts where payments can typically be expected within 1 month of invoices being presented. BEREC reiterates the relevance of contractual agreements between undertakings in the context of the fight against fraud and misuse. For this reason, it can be noted that very short payment terms could run counter to the effective withholding of money flow. BEREC would observe that no process is likely to be capable of supporting intervention within a 7 day period and therefore considers that undertakings entering into contracts which require payments to be made within short periods, such as the 7 days mentioned by Orange, may be exposing themselves to commercial risk in the event of fraud or misuse. BEREC would recommend that undertakings do not contract for outpayments in short periods such as 7 days. A time frame of 1 month from invoice may be considered by undertakings to be the minimum that would be appropriate.
94. ETNO goes one step further in the scope of cooperation and suggests that a common, central reporting process would enable the simultaneous reporting of fraud/misuse and alerting of both NRAs and operators to the relevant activity. Operators may then be in a position to better protect consumers by restricting or denying access to exploited services or numbers, in the limit of the technical feasibility and sustainability, so that NRAs would receive much faster notice of apparent abuse within jurisdiction. By a way of example, ETNO mentions that there are certain types of services that have been subjected to fraudulent activities to consumers, which, in turn, has caused generic consumer rejection to this set and full numbering range with very negative consequences to those who have nothing to do with the abuse or misuse. Moreover, when they migrate to less contaminated numbering systems they find that these new numbers are again used to commit fraudulent activities, again causing rejection by consumers to these new numbering ranges.
95. BEREC does not consider at this stage that including a centralised reporting system of the type envisaged by ETNO is appropriate. There are a number of reasons for this, which includes, inter alia, the difficulties to assure the accuracy of such records when the submission of such reports would be open to a large number of entities. The Consultation proposes an exchange of information between NRAs to register the cases reported under the BEREC cooperation process (therefore not all cases of fraud or misuse). This approach will ensure NRAs are kept abreast of the types of fraud or misuse that occur and will enable them to engage with stakeholders in the relevant jurisdiction on these issues. This position can be reviewed in the light of experience of the process. It should be stressed that the BEREC process is without

prejudice of the general application of the specific requirements for Member States and undertakings provided under Article 28(2) USD.

96. The GSMA remarks that in certain complicated cases of misuses or fraud, a series of requests must be initiated under the proposed process by the originating NRA to determine the true routing of the call. This information gathering phase will delay any payment withholding action at the terminating end of the call, which benefits the perpetrators of fraud and misuse.
97. BEREC agrees with this comment, which illustrates the need that all stakeholders involved in the process act swiftly.
98. Notwithstanding the foregoing, BEREC encourages coordination between undertakings through bodies of common interest, such as GSMA and welcomes other developments such as the work by i3forum pulling together the expertise of telecommunication operators[5]. BEREC also considers the institutionalisation of contacts within NRAs and undertakings as a useful instrument to benefit from the most efficient method of communication. Further, BEREC does not exclude the possibility of follow-up workshops with the industry in order to assess the functioning of the BEREC process and required improvements.

Withholding of revenues

99. Eircom warns that the effectiveness of withholding payments to prevent monetary gain for the fraudsters is vital. It is not clear how the BEREC Process will stifle the fraudsters' activities as they continually move locations and change their activities. The undertaking at the end of the chain, making the payments to the fraudsters, may be unaware of the illegal activity until well after the event, by which time the fraudster will be likely to have moved operations to another jurisdiction. This difficulty becomes more real when calls terminate outside of the EU Member States.
100. BEREC considers that this process, with the cooperation of undertakings within the EU will raise the profile of the issue of fraud and misuse and will in turn encourage undertakings at the end of the chain to take due diligence when dealing with terminating customers, service providers or operators. In particular, the process should aim to encourage even those parties outside the EU to have an incentive to put in place appropriate contractual conditions to help combat fraud and misuse.

Principle of thresholds

101. Representations from respondents were generally positive in respect of the principle of using thresholds.
102. In its comments, GSMA declares that Section 6.1.2 or the Consultation, paragraphs 168 and 169, describe how the application of retail charges by the retail operator, influences the NRA's decision to intervene. The measures described here may incentivise an operator to pass on the retail charges to the customer even in cases where previously the operator has decided not to do so. If the operator does this, the NRA may then judge the incident worthy of acting on and require the operator to withhold interconnect payment (removing the financial exposure of the operator to the fraud), whereas if the operator waives payment by the customer the NRA may take no action exposing the operator to having to pay the interconnect charges. Even

[5] http://i3forum.org/

if the operator has charged its customer (which may be a retail customer, but may also to be another operator earlier in the traffic chain from which it has received calls for transit/termination) there may be times when an operator and/or NRA would consider it appropriate to invoke the payment withholding process in order to disrupt the fraudsters, and then to encourage the refund of the operator's customer.

103. BEREC agrees that the situation described by GSMA cannot be excluded in practical terms. BEREC notes that responses by operators to the Questionnaire on Scale and Scope of the problem indicated that often end users are not charged for cases of fraud or misuse. In the responses it is also stated that in some cases, depending upon the circumstances, end users will be charged for the full retail amount or some other amount. BEREC, whilst recognising this is a matter for national processes, considers that where the amount charged by an undertaking is the full retail charges or something between the charge the undertaking incurs and the retail charge, an NRA may consider whether such a charge is appropriate when deciding whether to act to support that incident or future incidents relating to that undertaking. Having considered this point further, in order to facilitate the effectiveness of the fight against fraud affecting end-users pursuant to article 28(2) USD, and in the context of the Guidelines, BEREC proposes to change the recommended threshold from the retail charge to the wholesale charges of the retail undertaking.
104. ETNO remarked that "In general it is better not to specify precise thresholds basing upon which to take actions, since in different countries, and at different times, fraud and misuse may involve different amounts of money. It would be better to leave it up to each NRA, based upon national situations, to decide whether there is a case of fraud or misuse".
105. FCS noted that thresholds will have a different impact on larger and smaller operators and that a threshold would suggest a level which would inform fraudsters of a ceiling to which they could operate without intervention by NRAs. Eircom and Telecom Italia also put forward this second point and it was one of the comments made by GSMA.
106. GSMA noted that there is no single view amongst mobile operators about the proposed threshold noting that there are views supporting the thresholds and views suggesting other thresholds should apply.
107. A Respondent suggested alternatives to financial thresholds by using the number of calls to suspicious destinations or services within a defined time period.
108. BEREC notes the support for the principle of thresholds and has considered the points raised by these respondents. BEREC agrees that there is a perceived risk that by setting thresholds we are potentially signalling that there is a level of fraud or misuse that would not be acted upon. In practice this should not be a real concern if the levels are set such that the threshold does not make it cost effective for a fraudster to invest in the effort associated with such cases. Also, it is important to note that the figures are guidelines only, without prejudice to the general obligations and requirements pursuant to Article 28(2) USD and the associated national transposition, and this does not preclude the national bodies taking action if, for example, they consider that there are cases which are exploiting the principle of thresholds. This is therefore consistent with the suggestion by ETNO of leaving it to individual NRAs to decide on whether intervention is appropriate, based on national circumstances.

109. The suggestion to use an alternative to financial impact has some merit, as the financial impact can vary depending upon the charges which the undertakings apply for the calls. For example, a retail undertaking may choose to offer a reduced charge to an impacted end user that is the victim of fraud or misuse.
110. Having considered this suggestion BEREC feels that the level of complexity with the establishment of thresholds for different destinations, each of which could have a different financial impact, would be too complex to administer and therefore does not consider it appropriate to include this approach.
111. CWW expressed the view that "… participants would benefit from a common and harmonised procedure that provides guidelines for each NRA to follow justifying the threshold for regulatory intervention or interconnect payment freeze. This should certainly include thresholds…". Also, Verizon noted that "We strongly feel that national processes should be consistent and there should not be variation in the way this is approached in different jurisdictions. Ultimately it will result in the overall process being far less efficient, and runs entirely counter to the aims of the provisions."
112. BEREC considers that whilst not falling under the competence and scope of the present guidance a more prescriptive process in the area of thresholds and appropriate use of Article 28(2) USD would provide more certainty, but such certainty would have the impact of reducing the flexibility of an NRA to implement the obligations and requirements in the light of the specific national circumstances, such as the level of incidents in that particular jurisdiction. Furthermore, a more prescriptive approach would also provide more certainty to the people who are responsible for the fraud or misuse.
113. Given the responses received BEREC is of the view that the proposal to recommend non binding financial thresholds to NRAs as a consideration when deciding to investigate an incident as outlined in section 6.1.2 of the consultation paper is appropriate.

Level of thresholds

114. While there was a broad agreement around the principle of thresholds there were a number of representations made in the context of the appropriate level of thresholds to be applied.
115. Verizon expressed a view that the proposed thresholds are too low as the number of interventions that would result would be disproportionate. Their view is that "As a B2B provider we would expect to see a significant amount of revenue involved before it was withheld, either from us or by us."
116. Also Verizon stated that "we do not consider that the threshold should be anywhere near the administrative costs, and this comment by BEREC appears to suggest that such costs should be taken into consideration in setting a threshold. We consider that benchmarking thresholds against this sort of parameter would lead to a floodgate of cases which NRAs have neither the resources nor time to process effectively."
117. These comments appear to suggest that with the proposed thresholds there are a significant number of incidents that would be investigated. From the limited experience of the NRAs in BEREC it is not clear that the number of such incidents would be unmanageable but BEREC does intend to monitor the level of incidents and the threshold could be reviewed based upon experience.

118. Eircom notes that “There are operational matters that the final Process needs to avoid. In particular the gathering of information can be time consuming and resource intensive. Providing reports and additional information for use by ComReg, other NRAs and BEREC may prove to be a significant burden. The appropriate level of the threshold is crucial in this regard”
119. BT expressed the view that it “agrees that thresholds should be calculated at a Retail Level in relation to the cost of a fraud to an end user.” It also stated that “BT does believe that there will be significant resource costs incurred to monitor for fraud and misuse, to gather information and to withhold payments.”
120. BEREC notes that a fundamental aspect of Article 28(2) USD is to protect end users interests and rights. Whilst there is the issue, as discussed below, around the need to ensure that end users have an incentive to ensure appropriate protection of their systems, it seems reasonable to BEREC that thresholds that recognise the potential impact on the end user should be used but as explained earlier, BEREC has concluded that wholesale costs associated with the retail operator should be used for this purpose. BEREC is of the view that an undertaking should have systems or processes in place which enable call records for calls on its network to be readily analysed in the way necessary to provide the information needed to progress these investigations. BEREC notes that BT’s statement is consistent with this view although not all respondents agree. BEREC also considers that even with efficient systems there will still be some cost associate with the management of the investigations of fraud or misuse. While such costs are the type of costs which are come under the general area of fraud management BEREC would aim to have thresholds set such that the number of investigations does not swamp such processes.
121. Telecom Italia notes that the process appears to represent “a customer centric view document, while the greater impact is usually at operator’s expenses”. BEREC notes the existence of fraud types where the impact is on an undertaking as the fraud or misuse is perpetrated by the end user. The process is not intended to exclude such scenarios and the application of Article 28(2) USD in such cases would primarily depend on the conditions of the national legislation transposing EU law. Telecom Italia also notes that interconnect contracts sometimes include clauses for withholding of small sums each year without formal dispute processes being triggered. The amount to which Telecom Italia refers is €5,000 per annum but in BEREC’s view it is possible that instances of fraud or misuse may exceed this level therefore such clauses may be best reviewed to recognise traffic which is the subject of Article 28(2) USD requirements being made.
122. Eircom notes that it “agrees with the thresholds as outlined and in particular that only incidences in excess of a €5,000 impact should be investigated”. This is a slight misunderstanding of the proposal as it also suggests a lower limit of 3 times the customer bill or €1500 whichever is the higher. i.e. where a customer’s bill is normally €700 per month and the resultant bill relating to the incident is €2,500, this would be within the threshold. If the resultant bill was €1,500, this would be below the threshold for this end user but would be at the threshold for an end user whose monthly bill was typically at or below €500. In this context BEREC would note that the approach is based upon retail charges the customer would typically expect in a months against the wholsale costs, as outlined in paragraph 103.
123. Eircom also notes “There are frauds that are of low impact on individual end users, but occurring on a wide scale with the aim of bringing substantial benefits to

fraudsters. Wangiri calling is a prime example of fraudulent practice which affects many end users and is profitable for fraudsters. Eircom believes that these frauds should be tackled regardless of the financial value of the impact."

124. BEREC would agree with this proposition in principle but again the scale of the incident and the impact on consumers will be considered at a national level.
125. GSMA notes that "it is the GSMA Fraud Forum's experience that fraudsters adapt their methods when new mechanisms are introduced to disrupt their activities and that they will find and exploit vulnerabilities in a business process or fraud control mechanism". In particular, GSMA considers that is likely that fraudsters will be able to continue to operate profitably below thresholds without fear of intervention by perpetrating an increased number of fraud incidents with a lower associated value per incident.
126. BEREC agrees that these potential vulnerabilities need to be addressed, through a consistent and effective implementation of the proposed process by all NRAs. However, it is unlikely that the fraudsters may take advantage of thresholds mentioned as guidance in the consultation since the competence of NRAs to intervene under Article 28(2) USD in cases that fall outside the thresholds within the BEREC process has specifically been mentioned, notably in the situation where the form of misuse involved will be of a very low value to an individual but could be applied to a significant number of end users and the aggregate amount may be significant.
127. In summary, with the exception that the thresholds will be considered as wholesale costs, BEREC proposes to maintain the recommended thresholds as documented in the process as guidelines for NRAs, and as stated above without prejudice to the general obligations for Member States and national authorities to establish the specific requirements at national level pursuant to Article 28(2) USD. BEREC may however consider whether these thresholds should be reviewed when it has sufficient experience of the application of this process and would note that thresholds are only one consideration as to whether to take action in relation to an incident.

Incentives

128. GSMA considers that when legitimate customers are affected by fraudulent schemes (e.g. Wangiri calls, PBX hacking), undertakings usually also suffer a financial loss, often accompanied by loss of customer goodwill and reputation damage.
129. BEREC agrees that instances of fraud or misuse can have negative impacts on all stakeholders and hence there is a need for a process such as considered by BEREC for Article 28(2) USD.
130. GSMA maintains that the operator in the traffic chain with the retail end user as its customer has the greatest incentive, relative to other parties in the traffic chain, to support the proposed process, as it currently suffers the full loss if the end user is fraudulent, and it usually suffers part of the loss even where legitimate end users have been defrauded (e.g. through Wangiri calls or via PBX hacking). There are incidents in which a transit operator may also suffer a loss (e.g. in the case of a dispute with retail operator). The terminating operator in the traffic chain usually currently get paid by the previous party in the chain regardless of whether the traffic was fraudulently generated or not, due to the absence of payment withholding clauses in their bilateral contracts.

131. BEREC agrees that the parties in the current situation that are most exposed to fraud and misuse would be end users and retail undertakings, depending upon the type of incident. As such end users and retail undertakings are most likely to welcome this initiative. In BEREC's view, these are not the only stakeholders that should welcome this process as it should be in the interest of industry generally to see fraud and misuse tackled, rather than an acceptance that this is a fact of the industry which need not be tackled.
132. Verizon, GSMA and BT raised points in respect of the implications this process will have on stakeholders and the associated incentives for their efficient detection and handling of fraud. It was suggested by Verizon that Retail Operators, i.e. those undertakings that were directly providing service to an end user should not benefit from recovery of charges from an end user whilst also having the requirement not to pass on revenues associated with interconnection or services. If the Retail Operator did recover such charges it would benefit from the process. They also stated that the Retail Operator should be strongly incentivised to secure their systems and to encourage end users to do likewise.
133. GSMA also suggested that there is a risk that operators may have little incentive to invest in more effective fraud detection systems.
134. BT also suggested that "clarity is required in regard to minimum security requirements, both for end-users and for Communication Providers to detect".
135. BEREC agrees that it would be inappropriate for a retail undertaking to recover its charges at the retail level and also have the benefit of being required to withhold revenues from the next undertaking in the chain. BEREC also agrees that it is important to encourage all parties in the chain to take appropriate measures for protection against fraud and misuse.
136. Verizon suggested that where an operator experiences repeat instances of fraud or misuse this should be considered by an NRA when deciding on whether to take action.
137. BEREC is conscious of the risks of distorting incentives however until more is done to reduce the risks or improve awareness this level of intervention is likely to be necessary. It should be noted that NRAs have a margin of discretion as to whether to intervene and this should maintain appropriate incentives for stakeholders. BEREC would also agree with Verizon that where a body suffers repeat instances of fraud or misuse, through its own lack of action, this may be a relevant consideration for NRAs. An example may be an undertaking that offers a service to end users that has been the subject of repeat cases of misuse or fraud, such as international call forwarding being abused with no attempt to put in place appropriate security.

Consideration of the use of Article 28(2) USD

138. Verizon stated that they "are concerned by the signals that BEREC sends at paragraph 162, that where requests for revenue blocking [by the next NRA in the chain] are not being progressed, this should be communicated to the requestor with a justification." They suggested that NRAs should act with a bias against using these sensitive powers unless there is a compelling case to do so – and there it should not need to justify the non-use of them.
139. BEREC considers that it would be beneficial if an NRA communicated the reason why no action was taken as it will help inform other NRAs and BEREC of possible issues with the end to end application of this process. In addition BEREC notes that

when a national authority considers it inappropriate to use the powers to block revenues there will be an impact on one or more undertakings in that jurisdiction as revenues will be potentially withheld from it which the relevant national authority has not considered it appropriate to require the undertaking to withhold revenues from undertakings further down the chain. In this regard it may be that undertakings would encourage the relevant national authority to take action.

Article 28(2) USD impact on existing contracts

140. CWW noted that "paragraph 183 of the consultation document states "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) USD where possible." In this regard CWW would like to seek clarity as to whether and how each NRA would apply these powers directly onto contractual clauses. CWW stated that it is important to note that rendering such clauses ineffective through the use of Article 28.2 USD would be a major change to the standards currently applied in transit contracts. Given this considerations CWW urges BEREC to define and agree a more detailed and binding process with a clear view of whether clauses will be automatically rendered ineffective or fraud liability should be adjusted in inter-carrier agreements at a bilateral level.
141. BEREC recognises that the withholding of revenues in the case of fraud or misuse may not be covered in interconnect contracts, and on occasion such contracts may note that such action is not acceptable under the contract. BEREC notes that such a contractual clause regarding payments does not preclude a relevant authority from taking action under the relevant legislation relating to Article 28(2) USD such as requiring payments to be withheld. BEREC is aware that beyond the EU it is possible that relevant authorities do not have equivalent legislation to Article 28(2) USD and therefore the withholding of revenues by undertakings which are not providing services in the Member States may only be possible through contract changes. Where revenues are being withheld from such undertakings by undertakings within the Member States BEREC considers that the commercial pressures to make the necessary changes to the contracts will encourage them to make the appropriate changes.
142. ETNO notes that "as a general comment it is important that BEREC consider that operators have a very small and marginal possibility to deal contractually with the misuses and/or frauds caused by foreign commercial entities and/or providers: in fact, the contractual measures cannot have a great legal value or power in the case of such situations and/or cause lengthy legal conflicts between different undertakings with difficult practical solutions."
143. BT noted that it is concerned that the proposals in this consultation do not make adequate provisions for NRAs to address fully the complex cross-border contractual relationships that are in place between originating, transit and terminating operators. BT considers that there is a need to bring a higher level of control over the onward payments of call revenue, but due regard must be given to contractual undertakings which often prevent payments being withheld.
144. GSMA notes that "the process proposed by BEREC needs development and amendment to maximise the likelihood of success. Payment withholding is a powerful

tool in the fight against fraud and misuse, but it must be used appropriately. NRAs must avoid the risk of undermining confidence in the international interconnect framework and triggering commercial disputes as a result of the payment withholding element of the process. Such disputes could ultimately lead to the cancellation of interconnect contracts between operators and transit carriers, potentially reducing competition and access to services by consumers and increasing costs".

145. BEREC recognises that there are a wide variety of contracts relating to the conveyance of this form of traffic between operators and carriers. BEREC believes that the most effective solution for addressing the issues of fraud and misuse will be through such contracts, but as clearly demonstrated in the responses by operators and carriers, these contracts are currently part of the problem which impacts on the ability to stop the flow of money or traffic which relates to fraud and misuse. Consequently BEREC considers that the regulatory approach to requiring the withholding of such payments as identified on a case by case basis is the best short term approach to this whilst encouraging industry to revisit the relevant contracts.
146. BEREC would provide support to initiatives from the industry, in the relevant European fora, to work on these contractual issues and to set common contractual standards for the undertakings in Europe.
147. CWW does not fully agree with the sentence stating that "Withholding revenues on the other hand will reduce the financial exposure for end-users and operators in connection with the calls already made" (Paragraph 70). Although there are cases where the chain of requirements to withhold payments may protect carriers from financial losses, international (transit) operators and receiving parties are put at much higher risk, as their ability to benefit from the chain of interconnection payment freezes is potentially impacted by rules and regulations that differ to the new BEREC procedures and rather follow international standards maintaining liability for fraudulent traffic with the originating carrier in a transit agreement.
148. With regard to CWW's comment, and as outlined in paragraph 26 of the document subject to public consultation, BEREC's proposed process intends to take into consideration the interests at all levels of the chain. BEREC takes the view that the implementation of the process should run in parallel with the appropriate contractual measures to harmonise the obligations of undertakings in cases of fraud or misuse.

Revision of Contracts

149. TUFF noted that its members, both those providing fixed and those providing mobile connectivity and termination, have clearly identified the need to bring a higher level of control over the onward payments whilst accepting that cognisance must be given to contractual undertakings which often prevent payments being withheld. There is also recognition by members of the need, under various national and international laws, that control terrorist funding and proceeds of crime to ensure that telecommunications are NOT used as an avenue to transfer funds thus bringing members into conflict with these laws and regulations. TUFF considered that an introduction of a specified delay before any payment is made could provide a period of opportunity for NRA's to intervene where fraud or abuse has been detected.
150. Vodafone notes that national contracts often include the provision for withholding or disputing payments relating to fraud. These processes are believed to have reduced the numbers of instances of fraud and the value of the fraud at national level Vodafone and other respondents agreed that generally such clauses do not exist in

cross border contracts. Eircom notes that such clauses would in their view be beneficial and states that it is currently reviewing its relevant agreements, and intends to ensure that appropriate contractual provisions are included in its agreements as far as possible. Verizon notes that “as new contracts are generated, or existing ones are revised, we are taking steps to incorporate the provisions of Article 28(2) USD in order to ensure that we can address future requirements in the most efficient manner possible”.

151. Eircom believes that the introduction of industry guidance in relation to the inclusion of contractual provisions to reflect Article 28(2) USD would provide useful clarity and certainty in relation to the issue as between undertakings in the context of contractual negotiations. BEREC would suggest that the contracts could facilitate the withholding of revenues where action is taken by a national authority and further, to move to a scenario where this can be handled at a commercial level, rather than requiring such regulatory intervention. In addition contracts could reflect the requirement to refund revenues where payment has already been made in the case of fraud or misuse. This could be a similar model to that which currently exists in many national contracts.
152. Eircom remarks “that while Article 28(2) USD allows for withholding of payments relevant to fraudulent activity, operators may not always be in a position to successfully negotiate inclusion of contractual provisions in agreements to reflect the position under Article 28(2) USD. Eircom suggests that BEREC provide guidance in relation to this point so that there are consistent requirements EU wide in relation to contractual provisions”.
153. CWW suggests that the amendment of interconnection agreements will take time and this is not expected to change the industry as quickly as would be suggested by the consultation. CWW state that the changes are expected to take between 2 years (Europe) and 7 years (more difficult markets). Moreover, it is expected that not all carriers with which the company maintains or is commercially willing to set-up an interconnect agreement would agree to amended liability clauses in case of fraudulent traffic.
154. BEREC welcomes the views that contractual changes will help in this area and notes that these are already being explored by some undertakings. As detailed in the consultation, BEREC considers that ideally the process for intervention should be progressively managed as a contractual matter between undertakings (see paragraph 6 thereof). Therefore, BEREC would urge undertakings to bring forward any relevant contractual changes to facilitate a commercial process for management of fraud or misuse across borders and considers that, as this will be to the benefit of all parties, the process should be a priority for operators.
155. BEREC does not consider that it is in a position to advise on appropriate commercial contract conditions but would suggest that undertakings have sufficient clarity to assess the circumstances under which regulatory action may be taken and this should enable the development of relevant clauses in contractual negotiations. BEREC would agree with Eircom that commercial contracts could include the ability to refund payments for traffic in appropriate circumstances. This should reduce the problem of time pressures on undertakings in respect of investigations prior to payments being made.

156. In respect of a coordinated approach to this by industry, BEREC would suggest that recommendations could be developed by industry bodies as an extension to current work such as that undertaken in the area of fraud or misuse.

Operation

157. Eircom sees the Process proposed by BEREC in the consultation as “a welcome and necessary measure to enhance the arrangements currently in place to deal with fraudulent activity. The Process will expedite communications across Member States and ensure that action is quickly taken to block numbers and withhold payments relevant to fraudulent activity”. Eircom emphasizes “the need of a consistent implementation of the process across all Member States and suggests that standard templates for the collection and sharing of information be used by all National Regulatory Authorities (NRAs)”.
158. BEREC takes note of Eircom’s analysis and will discuss the development of such a template with industry in a future workshop.
159. CWW stated that there is a recognised need for further elaboration of a detailed process with clear and legally binding guidelines, to which operators can refer in their interconnection contracts. CWW also stated that it believes that a future process requires a higher level of standardisation of national and particularly cross-border activities, more (legal) certainty and clearly defined responsibilities, as well as some structures governing the end-to-end process and the achievement of objectives.
160. ETNO remarked that there is still ambiguity about the responsibilities of operators. Moreover, additional guidance is needed around the definition of fraud and misuse in the specific case of the national premium services numbering, and how requests to intervene would be dealt with practically.
161. BEREC considers that the identified scenarios of fraud or misuse includes AIT, as reflected in the final BEREC Guidance paper, and as such addresses the issues of inflated calls to premium rate numbers considering the protection of end-users as its fundamental aim, in accordance with Article 28(2) USD. The responsibility of undertakings will be to provide information as requested, to block numbers as requested and to withhold revenues as requested. In a wider context, undertakings should be looking to develop an industry process to address fraud and misuse on an end to end basis.
162. Verizon considers that without a properly harmonised process across the EU, including the test for fraud / misuse, they do not consider that those wishing to combat fraud will achieve their objective.
163. BEREC considers that the proposed process will provide much of the requirement identified by CWW, ETNO and Verizon with the final aspects being provided by the specific national processes to be implemented by relevant authorities. As noted in the consultation, BEREC does not consider it appropriate to attempt to define fraud or misuse and has taken the approach of identifying a non-exhaustive list of examples of fraud or misuse for consideration in national legislation transposing EU Directives.
164. TAG stated that they believe that the process outlined in the consultation would “be harmful to the telecommunications industry as it disrupts relationships between communications providers and undermines commercial confidence in the interconnect payment chain”.
165. BEREC does not agree with TAG’s view as it believes that it has been shown at national level in some Member States that a contractual process can be put in place

in respect to artificially inflated traffic (AIT) which has been positive for consumers and industry. This contractual process is the form of solution which BEREC would like to see industry moving towards and the proposed regulatory process in the consultation is an interim solution which aims to achieve a similar result to what could be achieved through such a process although a contractual process would have a number of advantages as indicated in this document.

166. Respondents to the consultation were mainly positive in respect of the process that has been proposed although most respondents had suggestions which they felt could offer improvements. Orange noted that national processes would have to take into account that perpetrators of fraud or misuse often have a very detailed knowledge of the general working practices within operators and service providers and observed that incidents often occur outside the normal working hours of national authorities.
167. BEREC notes this point but the detection and first line response to such incidents is with the undertakings concerned (or end users where appropriate) and BEREC would suggest that the relevant authority would typically be alerted to the incident after it had been addressed and would deal with the administration of the national process and Article 28(2) USD process during normal working hours. BEREC considers that the proposed process is the first step towards harmonisation and following the implementation of the process there should be a review of its performance to assess what changes or enhancements should be made.
168. ETNO also notes that generally only the NRA can order the numbering blocking and/or the withholding of interconnection revenue and that should be clearly defined in the new harmonized process. BEREC notes that in some jurisdictions undertakings may take action to block numbers at an operational level because of known fraud to or from these numbers, but where such action is permitted that would not be inconsistent with the proposed process as the relevant national authorities should also take formal action in the event of cross border issues.
169. Telecom Italia notes that in some cases the suspension of the payments chain has no effect on the suspension of the fraud, and suggests that this should also be reflected in the consultation document. It is possible that the relevant national body may consider that it is inappropriate to block numbers or require revenues to be withheld but this will be considered when the circumstances of the fraud are understood.
170. BEREC would note that the application of Article 28(2) USD will depend upon the circumstances of the specific incident.
171. The GSMA further notes that section 6.1.4, paragraph 182 of the draft report finishes, “An inability to disrupt the overall flow of money would not be considered as precluding the use of this process to the extent possible.” The GSMA requested clarification over this sentence and believes that if the process is unable to disrupt the money flow to the perpetrators of fraud and misuse, it should not be implemented. Also, Verizon is concerned that this statement implies that this process may be used regardless of whether it is possible to prevent the perpetrator from receiving the relevant revenue. Given the cost and effort that will be necessary to follow the proposed process, Verizon considers that it is not proportionate to use it if the ultimate objective cannot be realised.
172. It is BEREC’s view that although the implementation of the process may not, in some cases , and notably for earlier cases , allow the relevant authorities to disrupt the flow of money linked to a specific case of fraud or misuse, the process is still relevant as

one aim is to protect end users from fraud or misuse. Operators are encouraged to address the possibility of the regulatory intervention not being able to address the whole chain of payments by putting appropriate contractual conditions in place.

173. The GSMA stated that Member States should be entitled to evaluate whether the provision of accessibility to certain numbers in other Member States is correctly in balance with the associated risk of fraud and the real demand from the end users to access those numbers.

174. BEREC notes this point but considers that the issue is beyond the scope of Article 28(2) USD and is more relevant to Article 28(1) which is not in scope for this work stream.

Detail and clarification on the process

175. Respondents identified a number of key areas within the general proposal put forward for consultation that were considered important for the process to work effectively – these are discussed below.

176. In order to agree the process, a respondent argued for the detail to be reviewed with stakeholders in design sessions involving operators and/or industry associations. The GSMA also called for operators to be consulted.

177. BEREC is planning an implementation exercise, including a workshop with stakeholders. As part of this work, BEREC will be consulting on details and clarifying the implementation process. BEREC expects that the process will evolve and develop over time and it is likely that considerable refinement will take place following its initial rollout as a result of learning from practical application. It is envisaged that consultation (both formal and informal) between NRAs and operators will take place on a national basis as the requirements of Article 28(2) USD and application of the process are embedded in national regulatory proceedings and this will input into BEREC's development of the process's operation.

Example scenarios where the process might be applied

178. GSMA considered that the example of the process in section 5.3.1 of the consultation paper was useful but showed only a simple scenario. It suggested that additional examples be provided setting out a range of situations where the process might be applied. In particular, an example showing international roaming for mobile telephony customers should be incorporated.

179. BEREC included the figure in section 5.3.1 of the consultation paper to provide an overview of the process for cooperation between relevant authorities under Article 28(2) USD. It is intended as a reference for the high level process for information sharing and cooperation and is not specific to any particular fraud or misuse scenario. It would not be possible to cover all scenarios and BEREC does not consider that including additional examples would be beneficial at this stage ahead of process implementation. BEREC considers that additional scenarios may be reflected in further updates to the process and following reviews with stakeholders, where experience of the process in operation can be reflected.

Type of information shared

180. GSMA asked BEREC to confirm the minimum level of information to be exchanged between participants in a case.

181. GSMA considered that the minimum set of compulsory data should include:

- the number(s) subject to the fraud/misuse;
- details of the first and last time when the fraud/misuse was detected;
- the criteria used to detect the fraud/misuse;
- the type of fraud/misuse that occurred; and
- the entity reporting the case.

182. A respondent considered that Call Detail Records should not be required at the point of reporting the case.

183. BEREC agrees that there would be benefits for parties involved in the process if there was a common understanding of the type of information that needs to be shared. The information suggested by GSMA as set out above provides a good basis for the information that is likely to be relevant. BEREC would expect that the minimum requirement for an NRA to consider a case would likely be the information supplied on Call Detail Records, which would provide the origination and termination numbers involved in the fraud/misuse plus call details (i.e. date, time, call length and destination). In respect of the information exchange between undertakings and NRAs, as well as between NRAs, the precise detail may vary from incident to incident but typical requirements will include:

    a. A free text description of the incident
    b. Details of customer and retail undertaking
    c. Details of interconnect undertaking
    d. Call details including (Excel spreadsheet or similar):
        i. "A" Number
        ii. "B" Number
        iii. Time of calls
        iv. Duration of call
        v. Value of calls

184. BEREC considers that standardisation in information sharing may be developed through discussion with stakeholders following implementation of the process, when experience would inform understanding of the information that needs to be included to initialise and further investigations. BEREC is planning a workshop as part of its implementation exercise for the process and the development of an information sharing requirement is likely to be a subject for discussion.

Practical issues/ establishment of a common format for notifications and information exchanges

185. The GSMA and Eircom invite BEREC to promote the establishment of a common format for notifications and information exchange. The GSMA note in particular "if operator reports were made in a common agreed format and reported simultaneously to originating and terminating NRAs, the terminating NRA could, in the interests of speed and in cases where short-stopping or hijacking have not occurred, issue an interim freezing notice whilst the facts are confirmed and reviewed and a decision is made".

186. Eircom notes that it "is essential that a robust communications process be put in place. The effectiveness of any process will depend to a large extent on communications to provide initial notifications, progress reports and conclusions to NRAs and operators. Telephone contact will also be crucial for the key stakeholders involved in each event, to ensure that early actions are taken. These notifications would operate in parallel with the Process and aid NRAs in taking more rapid actions. E:Mail alerts to designated contacts in NRAs and operators must be an integral part

of the process. The e:mails should follow a prescribed template providing standard information on the type of fraud or misuse identified, the countries affected, any actions taken, actions to be implemented and the identity of the lead NRA. If the fraud is identified as originating from outside the EU, the e:mail alert should state whether a NRA or BEREC will act as the lead. The establishment of a web-site by BEREC would be a valuable communications channel. This can be used to provide less urgent updates to all stakeholders. The web-site can act as repository for all previous fraud and misuse events that were channelled through BEREC and their outcomes. Information and guidance for NRAs and operators would be an essential feature of the web-site. The web site can also be used to maintain updated information on numbering allocations across the EU and beyond."

187. Eircom also suggests that "BEREC should consider the use of a mechanism, such as e:mail alerts, to notify all NRAs and operators of fraud and misuse incidents as they arise. These notifications would operate in parallel with the Process and aid NRAs in taking more rapid actions."
188. BEREC takes notes of these comments and acknowledges that the use of a common format for cases notification and information exchanges would be useful in order to facilitate and speed up the intervention of the concerned NRAs.
189. Regarding the establishment of a dedicated BEREC website that is suggested by Eircom, BEREC believes that the contact point for an undertaking that faces a potential case of fraud or misuse should be the relevant NRA, which will then coordinate with other NRAs and consider taking action. Therefore, there does not seem be to a need for undertakings to have access to a centralized communications channel that would be established by BEREC. BEREC does not therefore intend to establish a dedicated website of this type but will keep this under review.

Numbering management

190. Several stakeholders, including GSMA, BT, TUFF and Vodafone consider numbering resource misuse as a key enabler for fraud and call for a stricter control by national authorities over the assignment of number ranges and over the leasing of number ranges by number range assignees to third parties. In particular, the GSMA indicates that "where such leasing is permitted by the NRA, the original number range assignee should be required to notify the NRA of this, so that details of the affected number ranges and of the services available via those ranges can be added to the national numbering plan or made publicly available through some other means".
191. Some of these stakeholders also note that updated information about who uses a specific number (particularly premium rate numbers), and what services are associated with this number, should be publicly available.
192. BT also remarks that "BEREC should have powers to ensure that the allocation of Number Ranges is done transparently across boundaries. Up to date information relating to allocated number ranges and to whom they have been allocated, should be available within Member States i.e. allocated number ranges within an NRA's control should be made easily accessible by all NRAs from a single published source, for access by interested stakeholders".
193. Telecom Italia considers that the involvement of international coordination bodies would facilitate telecoms operators' task of correctly identifying both the type of numbering and the termination of calls on well-allocated number ranges. It therefore encourages BEREC to guarantee, at least at the European level, the provision of

official, updated and consistent Numbering Plans and to act as intermediary with the other international bodies (e.g. ITU) for the supply of these Plans outside Europe.

194. Verizon indicates that NRAs should "be required to publish and maintain an accurate numbering plan, which clearly shows what purpose the resources are assigned for, and that unallocated resources are not used within their jurisdiction or others."
195. GSMA also believes that numbering resource misuse is a key enabler for fraud. NRAs can help to address the issue of numbering resource misuse independently of the proposed BEREC process through stricter national number range management.
196. On the same issue, Eircom notes that "in order to limit the potential for unallocated numbers to be used strict management of numbering plans is essential. This is a matter for consideration by NRAs and undertakings alike. BEREC, through a web site can communicate information on numbering ranges that are validly allocated by NRAs of other bodies in the EU. Web site number information will also permit stakeholders to quickly recognise numbers that are not valid. This will be valuable for NRAs and undertakings to manage their own programmes and procedures to block numbers and quickly identify 'short stopping'."
197. BEREC notes that the publication of details of allocated numbers by NRAs is not consistent across all Member States. Respondents have suggested that consistency would assist with the determination of which numbers are allocated but BEREC notes that fraud and misuse occur with numbers that are unallocated, but also with numbers that are allocated and then short stopped, or numbers that are allocated but not in use by the assignee. BEREC considers that there may be some advantage in a common format for the publication of numbers but at this time BEREC does not propose to address the issue of consistency in the information on allocated numbers as part of this work stream but the issue may be reviewed in the future. BEREC points out that the specific requirements at EU level as regards numbering plans are established under the EU regulatory framework, notably through the requirements and conditions on numbering, naming and addressing pursuant to Article 10 of Directive 2002/21/EC (Framework Directive).

Cooperation with regulators outside EU and with other institutions

198. Several respondents underline that many fraudulent activities involve jurisdictions that are outside of the European Union, and therefore propose that once the process is established and operational, BEREC should start engaging with foreign regulators to extend the applicable geographic footprint. Eircom "urges BEREC to establish international links through the International Telecommunications Union (ITU), national regulators, police forces and other enforcement agencies. Once these links are in place they can be incorporated into the Process". Eircom also suggests BEREC to "fully explore preventative measures that can be put in place with national regulators and law enforcement agencies both within the EU and beyond".
199. FCS members "are pleased to see a robust process laid out, with the bulk of the process definitions imposed on the communications between Relevant Authorities, leaving the NRAs a degree of freedom to decide how they are best suited to interact with the Communications Providers in their Member State". However, FCS remarked that in a recent case, an operator was not able to intervene "because the Police were investigating this as a criminal offence, their specific request was that information was not shared or disclosed to other parties whilst the investigation was progressing. Such a request from a law enforcement organisation makes a great deal of sense in

the majority of cases, however, it is incompatible with the BEREC process unless each NRA establishes a clear framework for co-operation with the relevant law enforcement agencies."

200. ETNO remarks that "BEREC should also consider harmonizing EU action against numbering misuses and/or frauds with the analogous initiative from the ITU organization, for instance supporting in EU the application of the ITU-T global numbering misuses/frauds regulation."

201. Whilst the scope of application of Article 18(8) and the BEREC process would be limited to EU Member States, BEREC, within the scope of its competences, agrees that the proposed process, when operational, should be used as a base for cooperation with other bodies and encourages NRAs to cooperate on a bilateral basis where practical. Indeed, paragraph 114 of the document states that the process is designed to be workable across EU Member States but acknowledges the relevance of taking into consideration aspects and implication of such cases beyond the EU.

202. However, as mentioned in the draft report, it should be noted 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.

203. The draft report also recommends NRAs to establish and develop cooperation with the relevant law enforcement agencies. Regarding cases where the police or other law enforcement authorities cannot disclose information collected in the course of the criminal investigation, the report indicates that these enforcement authorities may still inform the victim that the case can be reported to the NRA in parallel of the criminal investigations.

Reporting cases to the police

204. Some respondents commented that the current process for reporting a case of fraud/misuse involving telephone numbers to police was a complex and time-consuming activity that would not encourage stakeholders' participation in the process.

205. GSMA considered that the procedure for reporting a case of fraud would need to be streamlined to ensure efficiency in the process. It suggested that NRAs identify a single point of contact for the police within their country and ensure that the contact is familiar with the BEREC process and is prepared to cooperate with police across Member States to tackle cross-border fraud.

206. A respondent considered that reporting a case to the police should be required only for certain specific cases and should not be a prerequisite for reporting a case of fraud/misuse to the NRA under the process.

207. BEREC anticipates that cases involving fraud would generally be reported to the police (or other relevant national authority) regardless of any guidelines on action put forward under the process. However, the requirement to do so to initiate a case for investigation under the process would be a matter for national implementation.

208. BEREC does not consider the suggestion that NRAs identify a single point of contact in their national police that is familiar with the process to be a feasible proposal. There is unlikely to be a single national point of contact relevant for reporting fraud cases and it would not be appropriate for BEREC to pass comment

on national police structures for handling the reporting and investigation of cases and how coordination with police in other countries should be conducted.

Creation of a central database

209. The GSMA regrets that the database referencing cases of fraud or misuse reported under the process would be confidential and believes that there should be some transparency in order to allow operators to assess the effectiveness of the process. The association also supports the creation of a "common, central reporting process", in order to be able "to report fraud/misuse and simultaneously alert both NRAs and operators to current activity via a broadcast model, subject to data protection legislation".
210. Telecom Italia states that each NRA should have at its disposal a sufficient number of case studies, useful to use as examples in the case of disputes between operators around what may be considered as fraud and misuse.
211. Telecom Italia adds that it would be of help if the process of cooperation between BEREC and NRAs should institutionalize a phase of sharing among all the NRAs of:
    - all the fraudulent and/or misuse behaviours known at the National and International level;
    - the corresponding enforcement actions, including contractual ones, implemented by several operators considered by type (fixed, mobile, transit, other); and its effectiveness.
    - the corresponding regulatory actions, also in terms of re-pricing of tariffs.
212. BEREC notes that the draft report provides that a centralized database will be created in order to register cases of fraud and misuses managed by NRA in each country. For security and confidentiality reasons, the access to this database must be reserved to NRAs. It should be noted that this database is intended as a tool to assess the effectiveness of the BEREC process from time to time and as a resource for NRAs to understand the evolution of fraud and misuse. It is not an operational tool to be used in relation to management of information towards undertakings as its accuracy cannot be guaranteed. However, the results of the evaluation of data could be discussed with undertakings in a future BEREC/industry workshop. This database will enable NRAs to see what forms of fraud and misuse have been identified in the various jurisdictions.
213. More generally, BEREC would support initiatives by the industry in order to facilitate the sharing of information between industry players.
