



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

16th November 2012

We would welcome any comments on the contents of this document which is also available electronically at:

<http://www.btplc.com/Thegroup/RegulatoryandPublicaffairs/Consultativeresponses/>

Comments should be addressed to Kath Embleton, BT Wholesale Regulatory Affairs Department, by e-mail to kath.embleton@bt.com.



Executive Summary

BT welcomes BEREC's proposals to improve cross-border co-operation in tackling fraud and misuse of telecommunications networks. The overall objective must be to prevent a) customers from being harmed or inconvenienced or b) anyone from benefiting financially from telecommunications fraud or misuse. Cross border arrangements between relevant authorities should be introduced such that incentives for acts of fraud are removed and NRAs are able to co-operate effectively to combat those instances of misuse that arise..

BT welcomes the development of a guideline procedure that supports the development of cross border controls by National Regulatory Authorities ("NRAs"). Such controls will help Communication Providers to address instances of fraud or misuse quickly, and act as a deterrent to further fraudulent activity.

However, we think that what constitutes telecommunications fraud and mis-use has been drawn too narrowly. In particular, we think that regulatory agencies need to consider the increasing number of cross border "nuisance calls and texts" sent in vast volumes, which customers continue to experience, which are difficult for national regulators to address on their own. We're not talking here about malicious calls, but those generally made by companies often indiscriminately to attract customers.

We are 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. 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.

While these proposed changes may improve the handling of investigations by NRAs, end users should also be made aware of their responsibilities in relation to security. Article 28 (2) should not be used as an excuse for end users not to develop or use relevant security safeguards and practices. Safeguards could include actions such as changing the passwords on their switch away from the default and regularly checking the log of calls made through the switch for unauthorised use.

When investigating cases of suspected fraud or misuse, NRAs should adopt a "follow the money" approach to identify who will potentially gain from any fraudulent activity within the value chain and to identify whether any payment has been made. 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.



Initial Commentary

BT welcomes the opportunity to comment upon BEREC's consultation. BT agrees that both fraud and misuse are serious and complex issues with a strong international dimension. As such, pan-European, and preferably global, industry wide solutions are needed to tackle them effectively.

However, we think that what constitutes telecommunications fraud and misuse has been drawn too narrowly. In particular, we think that regulatory agencies need to consider the increasing number of cross border "nuisance calls and texts" sent in vast volumes, which customers continue to experience, which are difficult for national regulators to address on their own. We're not talking here about malicious calls, but those generally made often indiscriminately by companies to attract customers.

BT supports the objectives of the harmonised co-operation guideline procedure and processes proposed by BEREC for NRAs. The proposed processes are intended to protect the interests of consumers, businesses, and Communications Providers by preventing perpetrators of fraud or misuse from benefitting from their behaviour.

BT would like to see the implementation of a process with the scope to ensure clarity in regard to the responsibilities of all stakeholders including BEREC, NRAs, End Users, Communication Providers, Carriers and Terminating Operators in relation to Article 28(2). We accept the difficulties in providing clear, harmonised definitions of fraud and misuse as criteria differ from country to country. However we believe that common ground should be identified, especially to avoid any ambiguity as to whether a scenario is covered within the scope of the powers held by NRAs under Article 28(2). An example of such a scenario could be when a Communications Provider contests, in an instance of suspected fraud, that the call traffic did not look to be unusual or excessive and it was carried as requested "in good faith."

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.

In order for the process to be workable in the global telecommunication industry we believe:

1. The scope of what is covered under Article 28(2) should be clear and defined. The guidance provided in section 3.2 (Para 50) of the BEREC consultation document, should be adopted by all stakeholders as minimum guidelines for the purposes of Article 28(2).

For this purpose and for the purposes of providing guidance in the context of Article 28(2), situations dealt with by operators and authorities that could qualify as fraud or misuse can be illustrated by the following examples:

- The use of numbers from blocks yet to be allocated by the relevant authority to make calls with the intention to defraud end users or that are a nuisance to them.



- Short-stopping¹ in the same country, in another European Union country or beyond European Union borders).
- The use of a service (provided via a telephone number) by an unauthorised third party to whom the number was not allocated, without the consent of the party to whom it was allocated (for example phone hijacking, or PBX hijacking).
- A breach of the European CLI rules such as masking the CLI for example, 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).
- The use of CLIs that, when displayed to and subsequently used by the called party to return the call results in a call that is not related to the initial caller.
- The use of CLIs that, when displayed to and subsequently used by the called party to return the call results in an inappropriate cost to the original called party and is such that the recipient of the call unfairly gains financially. Typically, these may be ultra-short calls, simply to drop the CLI, so recipients worry they have missed a call and return it.
- Artificial inflation of traffic. This refers to calls that:
 - are made, generated, stimulated and/or prolonged for the direct or indirect benefit of any entity operating, hosting or otherwise connected with a telecommunication service as a result of any activity by or on behalf of such entity.
 - result in a calling pattern which is disproportionate to the overall amount, duration and/or extent of calls which would be expected from a good faith usage; or an acceptable and reasonable commercial practice relating to the operation of telecommunication systems. Examples include such practices as:
 - Private Automatic Branch Exchange (PABX) software being modified by hackers to support transit of calls to foreign; fixed, mobile and satellite premium rate numbers,
 - scams designed to encourage consumers to call or text back (e.g. missed or short duration calls from international premium rates, non-geographic or other revenue sharing numbers) and
 - scams that generate calls or texts from the customer without their direct action and/or knowledge (– e.g. dialler scams, smartphone applications, virus or other mobile malware, texts generated without the user's permission).

¹Short-Stopping example: *Calls are routed through a high cost International destination when they are in fact terminated elsewhere. Therefore callers face excessive charges, typically when connecting to "Premium Services" such as competitions.*



- Potential customers' providing false information when signing up to electronic services. Identity theft (concerning final customers, but also manipulation of network parameters), internal/employee thefts, or cloning cards are other situations which operators face on a regular basis.
2. When an offending number/CLI has been identified, the number information in relation to the offence should be made available by the NRAs in an accessible single source.
 3. Timely intervention and action within a process, with agreed milestones, is key in these cases.
 4. Where money has been paid out as a result of a service and 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. Also fraud or misuse may not be identified until sometime after the fact and possibly not until an invoice is produced. 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.
 5. All Telecommunications companies who operate within the European Union, or who do business with companies within the European Union, should be bound by Article 28(2), with positive engagement by NRAs with parties outside of the European Union.
 6. NRAs should control the granting of rights of the use of National Numbering Resources and 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.
 7. NRAs, when investigating cases of suspected fraud or misuse, should adopt an approach which will identify who will potentially gain from the activity within the value chain and also identify whether any payment has been made. As such, where it has been identified that payments have been made, or likely to be made. Communications Providers should not be adversely affected e.g. in cases of Call Selling or Pre-paid services.
 8. 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), as per the guidance provided in Section 7.1.1 of the BEREC consultation document.

In drawing up any proposals, we need to ensure that definitions are not drawn so rigidly that agencies cannot act when new examples of fraud and misuse appear in the future.



Global Implications

This consultation has come ahead of the ITU-T's quadrennial conference which is scoping the ITU-T's technical work for the next 4 years, and the ITU's World Conference on International Telecommunications, reviewing the ITU's international treaty "International telecommunication Regulations" for the first time since it was originally signed in 1988. Though the use of numbers and combatting fraud are themes common to both conferences, BT believes that the proposals within the BEREC consultation demonstrate best practices that can usefully be shared globally to resolve such issues without reference to international treaties.

BT is fully engaged in the technical work within the ITU-T on combatting misuse of numbers, and not only supports the ability of operators to resolve alleged cases of fraud and misuse through unilateral action, but recognises that decisions as to what is (or is not) fraud is the responsibility of national legal frameworks. The reporting of the misuse of numbers is a complex issue, in particular because the information required by Communication Providers tends to be the first 7 digits of a number (and often less), to determine routing and charging information, rather than the entire number.

In order to combat fraud and misuse, there needs to be greater international transparency on which number blocks or individual numbers have been allocated, that are legitimate. This requires information to be published by national numbering authorities in a consistent and clear manner. BEREC has an opportunity to share best practices used by CPs and to facilitate processes that address the issues associated with mis-use of numbers.



ANNEX 1

Response to Questions

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

It is BT's view that the following should be considered by BEREC:

When investigating cases of suspected fraud or misuse, NRAs should adopt a “follow the money” approach to identify who will potentially gain from any fraudulent activity within the value chain and to identify whether any payment has been made. 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.

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.

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) should take precedence over contractual obligations relating to payment for fraudulent traffic, even traffic carried in “good faith.

In addition to the areas listed, 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 (IPRNs) offer very quick pay-out terms, often within 7 days.

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. This is necessary so that the relevant authorities have all the information to take appropriate action. United Kingdom companies using off shore call centres will be addressed under the UK Persistent Misuse Policy. However, non-UK companies suspected of fraud or misuse should be identified and any information passed to the NRA who will then be able co-ordinate action with the relevant international regulators.

Minimum expectations/security requirements for end users should be defined to ensure that responsibility for debt is not deflected by the end customer (switch provider/maintainer), as a result of Article 28(2).

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

The focus of this consultation and the areas covered above appear, in BT's view, 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.

These are causes of real consumer and CP harm. It would not, however, require the blocking of destination number ranges to address Subscription Fraud and PBX/Virtual PBX Fraud activity. Guidance and awareness of the minimum security requirements for end users would help to reduce volumes of incidents and the cost of managing disputes.

NRA intervention, working with CPs and Operators to identify those profiting would reduce incidents and clarify responsibilities in relation to charges incurred. Dealing with Revenue Share type fraud in isolation may result in a migration to, and an increase in, Call Selling to legitimate number ranges.

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

Although the responses within the consultation appear to cover a broad spectrum, BT has identified, as outlined earlier in this document, other issues which we believe that BEREC should consider.

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

BT believes that it should be the responsibility of the victim to report the crime to the appropriate Law Enforcement Agency and in turn report this to the appropriate NRA. This would be the customer in the case of a PBX hack or illegitimate use of a customer's service, or it would be a Communications Provider in the case of a Subscription Fraud.

BT also believes that this constitutes the basis for a process to implement the requirements of Article 28(2). However, the proposed process does require the buy-in of all stakeholders and must have clearly defined roles and responsibilities.

It is BT's view that BEREC and NRAs play a key role in implementing the process and obtaining agreement. Areas for concern will relate to contractual issues, complexity and the costs for stakeholders to implement the process internally.

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

BT agrees that thresholds should be calculated at a Retail Level in relation to the cost of a fraud to an end user. This should be used as the baseline throughout the value chain in



relation to the cost of the fraud, whether it be a “real customer” who has been impacted, or a subscription fraud in terms of unrealised revenue.

If thresholds differ at a transit level these should be set and agreed to ensure clarity. BT does believe that there will be significant resource costs incurred to monitor for fraud and misuse, to gather information and to withhold payments.

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

Although BT agrees with the statement above, clarity is required in regard to minimum security requirements, both for end-users and for Communication Providers to detect.

BT does have concerns with the compatibility of BT’s international contractual agreements with the proposed process to withhold revenue. BT’s contracts with international carriers (European Union and others) have no specific provision for revenue retention beyond an ambition for all parties to cooperate to identify and limit fraud and resolve disputes.

Within the consultation (section 183) BEREC suggest that in cases where contracts don’t permit withholding of call revenue “....action should be taken to render such clauses ineffective through the use of article 28(2) where possible.” However, it is unclear if NRA would have the necessary powers to put in place legislation which would override international contracts. This is especially the case where such contracts involve non-European Union contractual agreements.

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

Yes, BT has 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.

BT has also raised the issues in regard to Call Selling which is described in BT’s response to question 2 above.