



The Point
37 North Wharf Road
London
W2 1AG
United Kingdom

BEREC
pm@berec.europa.eu

November 15, 2012

Re: draft report on the Article 28(2) Universal Service Directive: A harmonised BEREC cooperation process

With reference to BEREC's public consultation issued on October 5, 2012 on the draft report on the Article 28(2) of the Universal Service Directive: A harmonised BEREC cooperation process, France Telecom – Orange shall hereby submit our comments to the consultation.

We shall also take this opportunity to express our full support of the consultation response submitted by GSMA.

Ad chapter 2. Introduction

Generally, the document reads as if Premium Rate Numbers are the biggest risk. PRN risk is not insignificant but fraudsters are currently targeting geographic numbers that are being hijacked or short-stopped. This is relevant because the practicalities of withholding payment in a hijacking or short-stopping fraud scenario are different to withholding payment from a licensed PRS provider in our view.

The ultimate proposal should ensure that incentives remain in place for operators to control their fraud. In this relation, it is important that everyone in the communication chain is able to work together and exchange information to fight fraudsters based on a simple and clear process.

Ad par. 10: The assumption seems here to generally be that the end-user is in good faith. This line of thought ignores the situation where fraud is committed intentionally. The focus is also on the NRA to communicate to undertakings providing electronic communications services to block, whereas the identification is likely to be made by the undertaking reporting the fraud to the relevant authority from which point, the provider would need a speedy reaction by the NRA.

Ad par. 16, 20, 31: We urge BEREC to ensure that for any proposals on processes recommended at national level is based on a harmonised solution across Member States. Such proposals would also have to take into account that fraudsters often have very detailed knowledge about the general workings within providers and thus, fraud may occur outside of normal working hours of national authorities. Scenarios such as this should also be included in the cooperation process.

In this relation, we would also like BEREC to consider different scenarios for instance where the call is to be directed to a country outside of the EU; a call is in transit via a non EU country; and where a call is originated and terminated within the EU but carried outside of the EU (most commonly via the United States).

Ad par. 17: In relation to withholding of interconnection and service revenue costs, the process should be adapted to the fact that agreements on payments can be based on an obligation to pay as shortly as within 7 days.

Ad par. 26: Fraud today is not specifically linked to PRN. With cases where numbers and/or number ranges have been hijacked and used for shortstopping, the end-user is the fraudster. In the case of shortstopping, the call never reaches the terminating operator, but may be stopped any time through the chain of operators (MNOs, carriers, fixed operators). The NRA in the intended terminating country will not be able to assist in stopping the fraud, as the call never reached his country. In such a case, it is important that the authorities in the country from which the call originated is able to work with the operator on short notice. We therefore recommend that specific service levels be defined for both national authorities and providers for the adapted to different fraud scenarios.

Ad par. 27: The consultations 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.", however there is little incentive for an operator to do this, in regards to retail traffic originated on their network, if they have a route through which they can block onward payment to their carrier. In fact, if operators 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.

Ad chapter 3. Article (28.2) USD issues

Ad par. 49-50: We find it relevant for BEREC to work on a dynamic interpretation of what constitutes a fraud or misuse scenario in relation to allowing an effective implementation of Article 28(2) of the USD. It should be without doubt that authorities should not stand in the way of allowing networks to block number ranges, which have been identified as being used for defrauding.

Ad par. 57-59: We support the proposal of BEREC to recommend that NRAs constitute first point of contact in the context of cross-border fraud or misuse cases referring to the necessity for BEREC to work with providers and NRAs to determine relevant service levels.

Ad par. 68: We believe that in order for measures to be effective, it is imperative that all designated authorities follow the same rules, i.e. if one authority allows an operator to withhold payment, then all authorities involved in the financial flow must apply the same ruling ("country of origin" principle). If rules vary across the chain of countries in which providers are impacted due to the call being in transit in multiple countries then operators/carriers risk being financially exposed.

This case becomes even more complex when the call is in transit in a non-EU country.

Ad chapter 4. Questionnaires issued during course of project

-

Ad chapter 5. Common process

Ad chapter 5.3: Whilst the proposal is based on the assumption that national authorities will drive the process, all of the work related to identifying transit carriers will fall with operators /carriers. It is mentioned that regulators need to act within a prompt timescale, however we would like to see a more complex example than the one in section 5.3.1 including multiple carrier businesses in different geographies and also parties outside of the EU so that scenarios can be worked through; and an example SLA for regulators, operators, carriers to show that this can be achieved with multiple parties within the payment timescales

In addition, it is not clear from the proposal whether operators are permitted to block number ranges that are identified as fraudulent. The proposal appears to be that the regulator in the terminating country will request blocking of numbers on a case by case basis. We believe that this will have no impact on hijacking / short stopping as the call would not reach the destination the number range was intended for.

We therefore propose that where we have evidence that a number range is a target to fraudsters, we want to be able to block number ranges - failure to do this will increase our overall fraud cost.

It should also be noted that in the case where the authorities have requested blocking of a number/number range, the operator would potentially only stand to benefit from the process, whereas the carrier could suffer quite badly financially. An impact analysis should therefore be conducted.

Ad chapter 6. Practical implementation process

Ad par. 168-169: These measures 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 regulator 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 regulator may take no action exposing the operator to having to pay the interconnect charges.



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

-

Yours sincerely,

Elin Nolsoe Nielsen
Head of EU Affairs
Group International Regulatory Affairs
France Telecom - Orange