

eircom Group

**Response of eircom Group to the
Body of European Regulators for Electronic
Communications (BEREC):**

**Consultation on Article 28(2) Universal
Service Directive:
A harmonised BEREC cooperation process**



16 November 2012

DOCUMENT CONTROL

Document name	eircom Group Response of eircom Group to the Body of European Regulators for Electronic Communications (BEREC): Consultation on Article 28(2) Universal Service Directive: A harmonised BEREC cooperation process.
Document Owner	eircom
Last updated	Final
Status	Non-Confidential

TABLE OF CONTENTS

EXECUTIVE SUMMARY 4

GENERAL COMMENTS 6

RESPONSE TO CONSULTATION QUESTIONS..... 9

 ARTICLE 28(2) USD ISSUES 9

 COMMON PROCESS 9

 PRACTICAL IMPLEMENTATION OF PROCESS 10

 ADDITIONAL COMMENTS 12

EXECUTIVE SUMMARY

eircom Group is pleased to have the opportunity to respond to this important consultation on a ‘Harmonised Cooperation Process’ in relation to Article 28(2) Universal Service Directive. eircom fully supports the proposals outlined to tackle fraudulent activity with a view to protection consumers..

eircom Group comprises eircom Limited and Meteor Mobile Communications Limited, referred to hereinafter “eircom”. eircom is the largest supplier of fixed line, mobile and internet services in Ireland. eircom provides a wide range of retail services to its consumer, business and corporate customers and is the largest provider of wholesale services in Ireland. In the context of retail and wholesale services, eircom is exposed to the many facets of fraud and misuse that are envisaged by Article 28(2).

eircom has for many years implemented various measures to detect and tackle fraud and misuse on its networks. However, the nature of fraud and misuse is continually evolving with the perpetrators becoming ever more agile and adept and therefore sophisticated measures for dealing with fraudulent activity within the industry are essential.

eircom communicates with its retail corporate customers on a regular basis, providing up to date advice on how to implement preventative measures. ComReg, the Irish National Regulator Authority, has also published Information Notices offering guidance to business customers.

When incidences of fraud and misuse occur eircom invokes its existing processes, which include advising and cooperating with ComReg.

The Process proposed by BEREC in the consultation is 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 wishes to highlight the following key issues in this response:

- The Process must be consistently implemented across all member states. Standard templates for the collection and sharing of information must be used by all National Regulatory Authorities (NRAs);
- Roaming fraud, which is not discussed by BEREC, should be dealt with as part of the Process. The nature of roaming fraud means that Process should aim to alleviate any delays in detection;
- Fraud and misuse activities are truly international in their scope, going well beyond the borders of EU member states. 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 considers that while Article 28(2) 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). eircom suggests that BEREC provide guidance in relation to this point so that there are consistent requirements EU wide in relation to contractual provisions.

In responding to the consultation eircom provides some general commentary and suggestions before answering selected consultation questions.

GENERAL COMMENTS

Roaming

The matter of roaming related fraud has not been addressed by BEREC. This is a particular area where fraudsters can expose weaknesses in the existing cross-border processes that are in place.

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.

International Contracts

eircom notes and supports the recommendations of BEREC in respect of the inclusion of contractual provisions in agreements reflecting Article 28(2) of the Directive. eircom is currently reviewing its relevant agreements, and intends to ensure that appropriate contractual provisions are included in its agreements as far as possible. eircom believes that the introduction of industry guidance in relation to the inclusion of contractual provisions to reflect Article 28(2) would provide useful clarity and certainty in relation to the issue as between operators in the context of contractual negotiations.

Management of Number Ranges

Number blocking is a key component in the toolkit for tackling fraud. The blocking of numbers immediately stops the fraudulent activity. 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 operators 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 operators to manage their own programmes and procedures to block numbers and quickly identify 'short stopping'.

Communications and e:Mail alerts

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.

Role of BEREC and Other Agencies

eircom notes and agrees with the BEREC comment that “...*that it is clearly in the interests of operators to prevent fraud and misuse.*”¹ Conversely it is an overstatement to suggest that “... *the primary capability to **prevent** (emphasis added) fraud and misuse lies with these operators and, in some cases, end users.*”² Operators and end users are the first parties to detect and identify fraud and misuse³. Based on experience and existing knowledge the operators can implement measures to prevent fraud and misuse.

¹ Paragraph 210 of the consultation document

² Ibid.

³ Are we saying here that operators cannot prevent fraud? We are not clear here.

Importantly it must be borne in mind also that other bodies, such as regulators and law enforcement agencies, have significant powers and roles to prevent fraud and misuse. These bodies can cooperate, share information and take legal action against perpetrators to prevent future fraud and misuse in a way that is simply not open to operators or end users. These other bodies can also develop contacts and procedures internationally going beyond the EU borders. BEREC should fully explore preventative measures that can be put in place with national regulators and law enforcement agencies both within the EU and beyond.

Process beyond EU Member States

Much of the criminal activity relating to fraud and misuse originates from outside the EU. This is beyond the scope of the proposed Process. Furthermore NRAs and BEREC do not have legal powers to follow the trail of fraudulent activities outside of the EU.

It will be important that BEREC lead discussions with international bodies such as the International Telecommunication Union (ITU), Interpol and other agencies to have as far as possible a worldwide agreed process in place. The purpose will be to share information, track the fraudsters, monitor patterns, identify new frauds and agree processes.

Through the ITU, Interpol and other agencies, BEREC can establish points of contacts around the world to speedily implement actions to block numbers, withhold payments and identify the source of the criminal activity.

While this would be time consuming and complex to implement, it would be an important extension of the Process.

Response to Consultation Questions

Article 28(2) USD issues

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 consultation document suggests that Premium Rate Numbers (PRNs) represent the largest fraud risk. In our 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.

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 operator 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.

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?

Common process

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.

In eircom's view the Process as outlined does represent a robust mechanism for NRAs to cooperate in order to tackle fraud and misuse.

It would be beneficial for NRAs and operators alike to have sight of the any information questionnaires / templates prior to implementation. This would ensure that an EU wide, consistent approach is attainable. It will be imperative to ensure that there will be compliance in the timely supply of information. Therefore the recommended timeframe for the supply should be set out and agreed.

As discussed in the response to Question 2, 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 must provide clarity on which NRA and operator will take the lead in tackling incidences of fraud against roaming customers.

It should be clearly set put that mandatory number blocking and withholding payments, on direction of the local NRA, is an integral part of the Process. This is necessary for the avoidance of any doubts and to guarantee that operators have their own procedures aligned with the Process.

In any event eircom agrees that all operators should have the ability to block number and withhold payments confirmed in their agreements, independent of any NRA direction to do so.

In order for the Process to have maximum effect it must be applied in exactly the same manner across all Member States. Difficulties may arise liaising with NRAs beyond the EU borders. It will be important therefore that BEREC lead discussions with international bodies such as the International Telecommunication Union (ITU) to have a worldwide agreed process in place.

Practical implementation of process

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.

There is a risk fraudsters will modify their activities to operate below a threshold once it is set and becomes known. This will prolong the period while their activities go undetected.

eircom agrees with the thresholds as outlined and in particular that only incidences in excess of a €5,000 impact should be investigated.

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 calling⁴ 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.

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.

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.

As stated above, eircom notes and supports the recommendations of BEREC in respect of the inclusion of contractual provisions in agreements reflecting Article 28(2) of the Directive. eircom is currently reviewing its relevant agreements and intends to ensure that appropriate contractual provisions are included in agreements as far as possible. However eircom believes that the introduction of industry guidance in relation to the inclusion of contractual provisions to reflect Article 28(2) would provide useful clarity and certainty in relation to the issue as between operators in the context of contractual negotiations.

⁴ A scam involving computer dialled random calls to mobile telephones. The recipients believe that they have missed a genuine call and return the call. The numbers are either premium rate or international numbers.

Additional Comments

Are there any additional comments in general or on remainder of the document?

To guarantee the efficacy of the national numbering plans each NRA, or the appropriate national body, must ensure that their plans are always up to date and maintained in all details. In addition, and to assist number blocking, the numbering plans should be publicly available to allow all other NRAs and operators to quickly determine whether numbers are valid. Nevertheless it may prove necessary to block numbers which are valid, when it is only possible to block entire number ranges.

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.
