Body of European Regulators for Electronic Communications

BEREC

BoR (19) 241

BEREC summary report on the Workshop on Fraud & Misuse of the E.164 number range

5 December 2019

Contents

Executive Summary **2**

1. Introduction **4**

2. Benchmarking from NRA Questionnaires July 2019 ..... **4**

3. Cyber Telecom Fraud Action - Europol **8**

4. CLI Fraud – BICS.com **9**

5. Overview of Fraud & Misuse of ECS - ComReg **11**

6. Insights to fraud & misuse of numbers, a suggested role for NRAs - EETT **12**

7. Panel discussion & Next steps **13**

Annex 1 ..... **15**

Executive Summary

1. In March 2013, BEREC approved BoR (13)37 "*Article 28(2) USD Universal Service Directive: A harmonised BEREC cooperation process. BEREC Guidance Paper*". That paper outlined a BEREC process for cross border regulatory cooperation in the intervention by the regulators or other relevant national authorities in cases of fraud or misuse. Included in the Report there was a commitment to monitor the practical issues around the process and to review the process as necessary.

2. In 2016 BEREC carried out the aforementioned review which included a short survey of NRAs' experiences of utilising the cross-border process and the reasons why, due to particular legal, procedural or practical reasons, NRAs may not have used the cross-border cooperation process. An internal document, BoR (16)226, was made available in 2016 that analysed the responses to the survey and the case studies allowed BEREC to make observations and draw some conclusions on the utilisation of the cross-border process in the future, including some recommendations for improving the effectiveness of the BEREC process for cross-border cooperation.

3. In October 2019 BEREC held an internal workshop titled "Internal Workshop on NRAs experiences in cases where E.164 numbers are used in cases of international (cross-border) fraud and misuse of Electronic Communications Services" in order to discuss NRA's recent experiences of cases of fraud and misuse and the cross border aspect of fraudulent connection fees.

4. The workshop attendees were BEREC members as well as a representative of Europol and BICS.com.

5. The first part of the workshop included presentations from the two independent speakers followed by one presentation from ComReg and another from the Greek Regulator, EETT. The presentations were followed by a panel discussion on issues related to fraud and misuse of the E.164 number range.

6. The workshop concluded with a panel discussion which focused on how cooperation between NRAs can be improved and how NRAs and the outside organizations such as Europol can assist each other in the management and enforcement of powers where necessary to minimize the fraud and misuse of the numbers.

7. It was agreed that the "End-user" working group is not the correct work stream for dealing with "The fraud and misuse E.164 number range", and therefore it was suggested that an alternative BEREC Working Group should be established in order to deal with this issue.

8. Following the workshop, a discussion was held within BEREC and it was agreed that a work stream would be created to address the issue of the access to a common EU number database that stores details of numbers for cross checking purposes.

9. In addition, it was also proposed the establishment of a new task force that could address other issues like:

    a. Slow inter-NRA response times.

b. Lack of automation when exchanging information.

c. Lack of access to the technologies used by those who perpetrated fraud and misuse.

d. The agreement of a common BEREC position on the description of what are cases of fraud and misuse.

e. Unification of the aims and methods of the various agencies and their approaches to the issues (e.g. NRAs, EC, BEREC groups, ITU, Europol, Operators, GSMA, Interconnection Carriers).

10. Another proposal was the establishment of a network of stakeholder in order to create a matrix of competent authorities and contact points with responsibility for Article 28(2) of the Universal Service Directive across Member States.

11. BEREC will take measures to create a consolidated list of premium rate numbers from European countries and to establish a list of contact points of those experts who are tasked to deal with this topic (within the NRAs), who would be ready to engage, if and when needed.

1. Introduction

12. The workshop was chaired by Ms. Therese Hourigan, BEREC Co-Chair of the End Users Expert Working Group, who opened the workshop and noted that the results of the questionnaire carried out by BEREC members had set the agenda for the workshop. Ms. Therese Hourigan anticipated that the workshop may highlight how BEREC members can take advantage of the experiences NRAs have had when managing the fraud and misuse of the E.164 number range and in particular on the EUROPOL and BICS experiences.

2. Benchmarking from NRA Questionnaires July 2019

13. In June 2019 a questionnaire was circulated to all BEREC member countries. The questionnaire was aimed at investigating how NRAs currently manage with abuses of the E.164 number range, and how related issues should be discussed at the 8th October 2019 workshop. Most of the responses are summarised below with the verbatim responses to questions 5 to 21 included in Annex 1.

14. In respect to questions on actions in relation to fraud and misuse and withholding of revenue, 7[1] of the NRAs responded yes and 8[2] no. In respect to resolving disputes between operators 7[3] NRAs offer a facility whereas 7[4] do not.

Figure 1 Answers to Q5

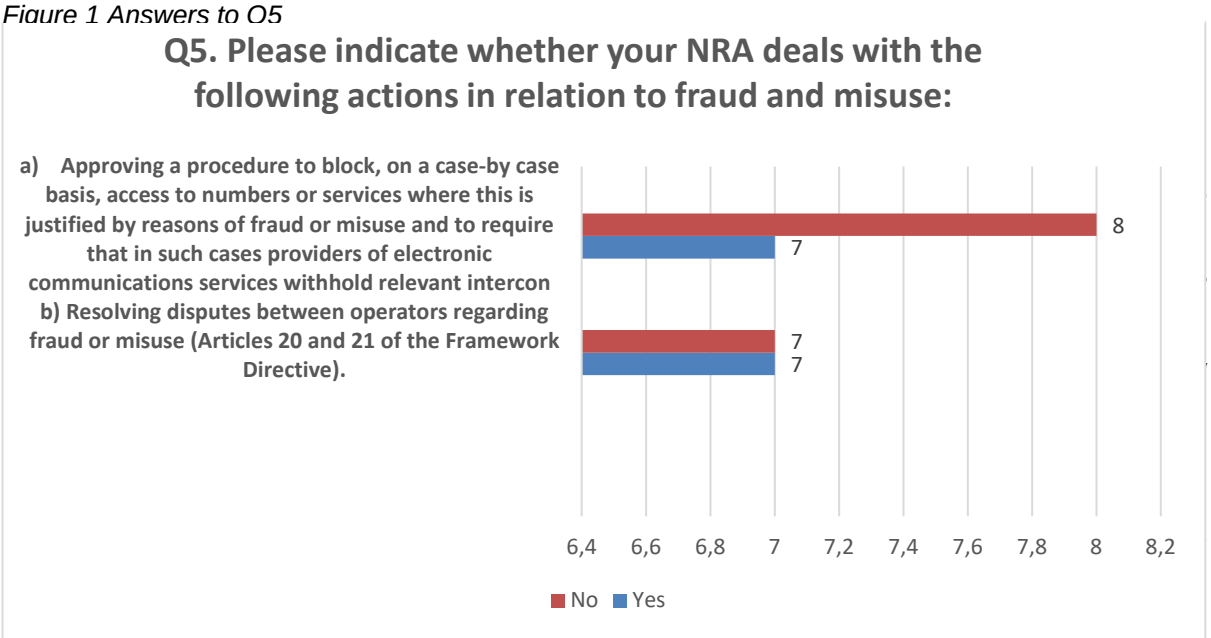
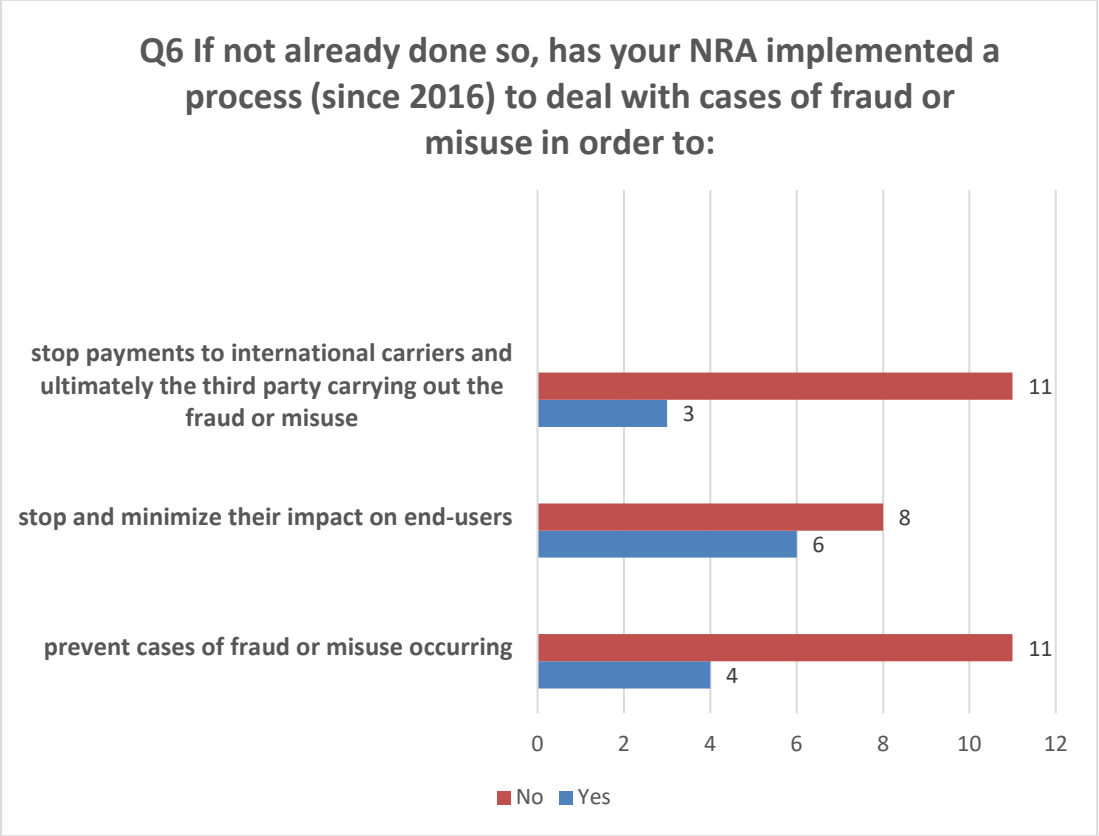


Figure 2 Answers to Q6

[1] , BIPT, BNETZA, MCA, NKOM, NMHH, OFCOM, SPRK
[2] AGCOM, AKOS, ARCEP, CNMC, COMREG, EETT, RRT,TRAFICOM
[3] AGCOM, AKOS, CNMC, MCA, NMHH, OFCOM, SPRK
[4] ARCEP, BIPT, COMREG, EETT, NKOM, RRT, TRAFICOM



15. Of all NRAs who responded to questions regarding the implementation of a process to deal with fraud and misuse

- BNetza, Ofcom and ComReg responded that they stop payments to international carriers;
- BIPT, Bnetza, ComReg, MCA, Ofcom, SPRK answered that they implemented a process to stop and minimise the impact of fraud and misuse on end-users;
- BNetza, NMHH, OFCOM and SPRK responded that they prevent fraud or misuse occurring.

16. NRAs who responded to question 8 on the financial thresholds indicated in BoR (13)37, BIPT, EETT and RRT answered that the financial thresholds set out in BoR (13) 37 are not set at a realistic and practical level.

17. In response to question 10, on the measures taken independently by operators to address and mitigate cases of fraud or misuse, the majority of NRAs (10[5] out of 13) answered that they are aware of measures taken by operators in their jurisdictions. However, in respect to question 11, on cooperation with other NRAs in cases of cross border fraud or misuse only 5[6] out of 15 NRAs answered that they have cooperated – full details are set out in Annex 1.

[5] AKOS, BNETZA, CNMC, EETT, OFCOM, NKOM, NMHH, RRT, SPRK, TRAFICOM
[6] BNETZA, EETT, NMHH, OFCOM, SPRK

18. In response to question 12 on the use of the provisions of Article 28(2) USD to block access to numbers or services and to require providers of electronic communications services to withhold interconnection or other service revenues at a domestic level, 6 NRAs (AGCOM, BNETZA, CNMC, COMREG, NMHH, OFCOM) declared to have used those provisions and 9[7] other NRAs declared to have not used them.

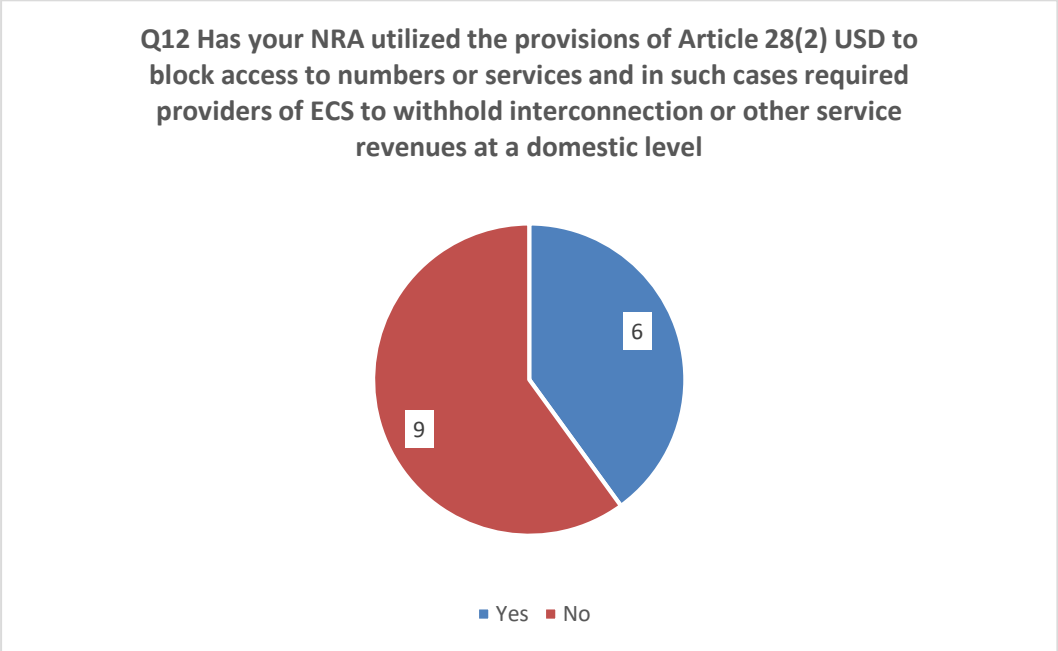


Figure 3 Answers to Q12

19. There were no reported cases of fraud not previously identified in Section 3.2.2 of BoR (1) 37.

20. The majority[8] of NRAs agree that more needs to be done to promote the benefits of the BEREC guidelines. In addition, NRAs[9] declared that a common data base of contact points for each NRA or relevant authority would assist in cooperation among member states on issues of fraud and misuse.

21. In addition, 10[10] out of 13 NRAs consider that a reference database with a register of cases of fraud or misuse reported by NRAs in each country, would act as a knowledge base for NRAs and would facilitate the review of trends and the effectiveness of the processes being undertaken.

[7] AKOS, ARCEP, BIPT, EETT, MCA, NKOM, RRT, SPRK, TRAFICOM
[8] BNETZA, CNMC, COMREG, EETT, NKOM, NMHH, OFCOM, RTR, SPRK
[9] AKOS, BNETZA, CNMC, COMREG, EETT, MCA, NKOM, NMHH, RRT, SPRK, TRAFICOM
[10] AKOS, BNETZA, CNMC, COMREG, NKOM, NMHH, OFCOM, RRT, SPRK, TRAFICOM

22. Two questions 18 and 19, on information to publish, a slight majority of NRAs agreed that blocked numbers should be included in a database[11], with the names of operators[12].

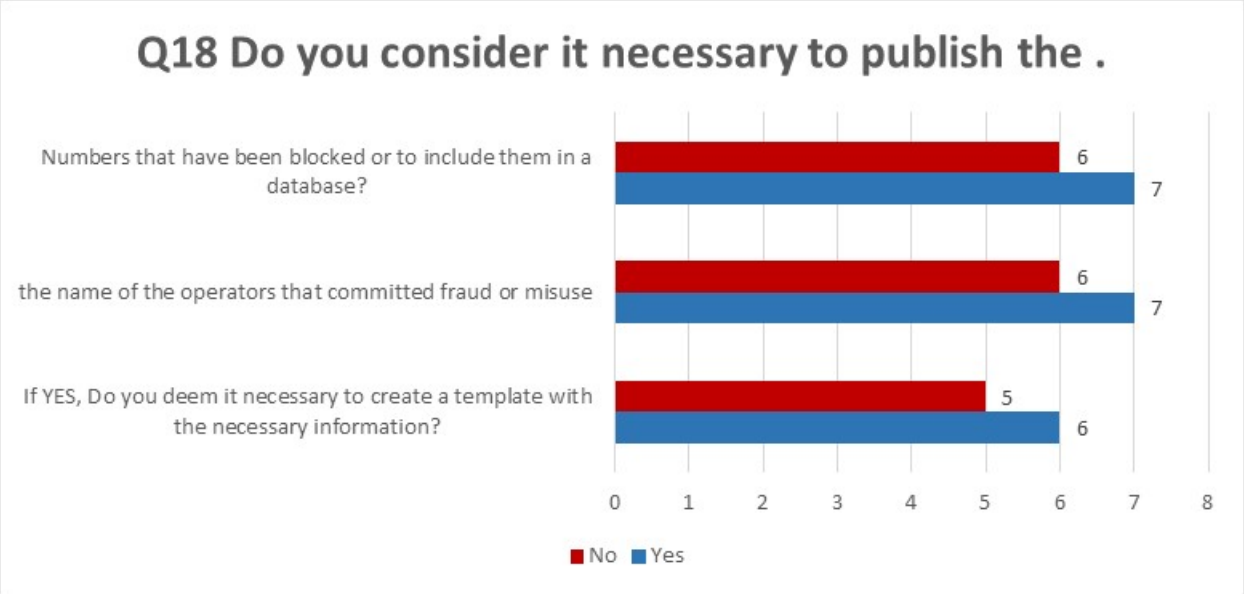


Figure 4 Answers to Q18

23. The majority of NRAs considered that some best practice guidelines would help to reduce the number of fraud and misuse cases in the future. This would also assist NRAs in dealing with cases ranging from contract clauses facilitating the withholding of revenue,[13] to raising standards in end user protection,[14] to cooperation with police and other enforcement and regulatory agencies[15].

[11] AKOS, BNETZA, CNMC, NMHH, RRT, SPRK, TRAFICOM
[12] AKOS, BNETZA, CNMC, NMHH, RRT, SPRK, TRAFICOM
[13] AGCOM, AKOS, BIPT, BNETZA, COMREG, EETT, MCA, NKOM, NMHH, OFCOM, RRT, SPRK, TRAFICOM
[14] AKOS, BNETZA, COMREG, EETT, MCA, NKOM, NMHH, OFCOM, RRT, SPRK, TRAFICOM
[15] AKOS, BIPT, CMNC, COMREG, EETT, MCA, NKOM, OFCOM, RRT, SPRK, TRAFICOM

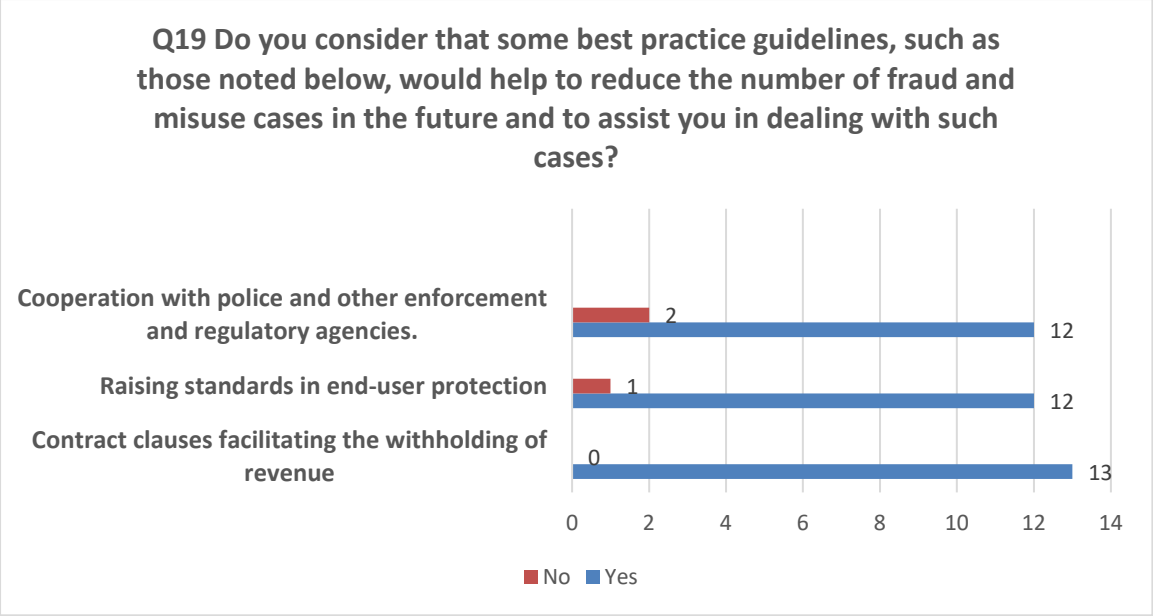


Figure 5 Answers to Q19

24. On the basis of the preceding responses, the following themes were agreed for the workshop.

    - Exchange of regulatory approaches and experience on fraud and misuse of numbers and services.
    - Practices and experiences that can be shared regarding cross-border co-operation.
    - Trends in fraud and misuse; approaches to authenticating and verifying calls, CLI Spoofing etc.
    - How to prevent blocking legitimate cross-border calls.
    - How to ensure NRAs can react quickly to reports of fraud and misuse, sharing of information and cooperation when operators hold Call Detail Records (CDRs) to enable call tracing.

3. Cyber Telecom Fraud Action - Europol

25. The first speaker, Mr Daniel González of Europol, gave a brief account of the recent fight against cybercrime. In 2013, Europol set up the European Cybercrime Centre (EC3) to bolster the response of law enforcement to cybercrime in the EU. Its objective is to coordinate police organisations of the different countries. In addition to law enforcement agencies, EC3 is open to and encourage public bodies in different EU countries and international agencies to cooperate with them.

26. Initially, the detection of behaviours was achieved by following the payment chain. This involved identifying the different carriers involved in the traffic. As the carriers were usually

in different countries, many police forces and prosecutors had to be involved. Therefore, it was considered that it was more effective to identify the International Premium Rates Numbers (IPRN) providers settled in one country, and to focus on them.

27. For this reason, it is essential to identify the operator who had been allocated the number involved in fraud. There are countries, such as Spain, that have information (numbering allocated operators) accessible on a web page[16]. For this reason, Europol requests BEREC members to facilitate these links in the different countries in order to quickly identify the responsible operator for each number.

28. These numbers that are involved in fraud are openly sold on social media websites. There is an independent expert who collects information on these numbers every year. Now, Spanish national police has promoted an initiative (supported by Europol) aimed at creating a similar database in collaboration with the University of Malaga. Through the latter, international coverage will be provided for the beneficiaries of all EU Member States (Public sector).

29. At the moment, it is just an initiative, however it has received a positive response amongst Europol participating countries. The support of BEREC would be useful and encouraging, providing the initiative with even more strength for further development.

30. Europol explained the operation of the database, the method of access and the type of information that is provided regarding the numbers that have been involved in fraudulent behaviour(s). Europol does not act on the complaint of individuals but at the request of the police of the Member States. For this reason, fraud must be reported by the operator to the police in the country where the crime occurred in order to create a registration number, this allows Europol to request further information. In each Europol member country, there is a contact person. If any NRA wishes to know the person responsible in its country, it will be provided.

31. In conclusion, Europol is creating a database, available to public bodies, of premium rate numbers and their operators. Europol requested links to the public access website containing operators and its allocated numbers in the different countries, if available.

4. CLI Fraud – BICS.com

32. The second speaker, Ms Katia Gonzalez Gutierrez of BICS.com, gave a brief background to BICS and its involvement with CLI fraud. BICS.com (BICS) specified that its mission is to "Deliver converging international wholesale solutions to existing and future communications service providers worldwide". BICS includes its main shareholder; Proximus and a further shareholder; TN Group (with 21 properties in Africa and Middle East) and provided the following details:

    - 1: 10 calls through BICS
    - 30% roaming through BICS

[16] https://numeracionyoperadores.cnmc.es/numeracion

- Global Fraud loss – 29.2 Billion Euro– 60% related to international fraud

CLI Spoofing – Voice calls

33. Calling Line Identification (CLI)[17] spoofing is the term used when a consumer receives a call that presents a number that is not the number of the caller.

34. CLI spoofing deliberately changes the telephone number and/or name relayed as the Caller ID information. This masks the identity of the fraudulent caller and mimics the number of a real company or person who has nothing to do with the real caller. This practice is financially damaging to carriers as potentially revenue is lost and BICS confirmed that there is an issue when numbers that are intra-EU and subject to roaming rates that are regulated appear as CLIs from outside EU.

Wangiri- Voice & SMS

35. Wangiri calls and SMSs abuse the end-users faith in the telco providers and industry in general as they are a nuisance and potentially financially damaging if a consumer calls the 'missed' number back. In recent example in the UK, O2 and EE users received up to 120 missed calls per hour. However, the fraud is not successful until the end user calls back. The nuisance of the calls may also cause end-users to switch providers.

36. Wholesale industry initiatives aimed at dealing with international calling fraud:

	Consumer Fraud	Network Operator Fraud	Carrier Fraud	
Frauds Impacting	CLI Spoofing – Bypass – Wangiri – Spam	CLI Spoofing – Bypass- Call stretching – IRSF- Short Stopping	Bypass- Call stretching - IRSF- Short Stopping	
STIR / Shaken	YES			SIP only, Centralized model, Certificate provider
Solid/ Seismic	YES	YES	YES	SIP & ISUP, No central authority, distributed model, forgets carriers
Block-chain	YES	YES	YES	SIP & ISUP, No central authority, distributed model, Cross-service inclusive

37. Operators, Wholesalers and Regulators could potentially provide "Multi-tiered" solutions:

- Deploy filtering platform
- Collaborate with other carriers and operators

[17] CLI means the number that can identify a caller.

- Provide a regulatory framework allowing international operators to work together on international solutions

5. Overview of Fraud & Misuse of ECS - ComReg

38. The third speaker, Mr Tom Boyce from ComReg, presented the scope of the discussion and clarified that fraud and misuse of electronic communications services (ECS) are generally perpetrated in two ways:

Single end-user	Multiple end-user
• High revenues o PBX-hacking o Roaming fraud	• Low individual revenues o PRS – Premium SMS

Current NRA Powers

39. In dealing with this type of fraud NRAs have the following powers:

Article 28 USD (Directive 2002/22/EC as amended by Directive 2009/136/EC) – Access to numbers and services

1. Member States shall ensure that, where technically and economically feasible, and except where a called subscriber has chosen for commercial reasons to limit access by calling parties located in specific geographical areas, relevant national authorities take all necessary steps to ensure that end users are able to:

(a) access and use services using non-geographic numbers within the Community; and
(b) access all numbers provided in the Community regardless of the technology and devices used by the operator, including those in the national numbering plans of Member States, those from the ETNS and Universal International Freephone Numbers (UIFN).

2. Member States shall ensure that the relevant authorities are able to require undertakings providing public communications networks and/or publicly available electronic communications services to block, on a case-by case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues.

Previous BEREC work on these issues

40. In 2010 BEREC issued a report on cross-border issues under Art 28(2) USD (BoR (10) 62 Rev 1).[18] The report identified the following key challenges arising from the revised USD (in transposition at that time):

    - Different competent authorities designated as a "relevant authority";
    - Concepts of "fraud" and "misuse" not defined;
    - Established NRAs approaches not defined.

41. In 2013 BEREC published a guidance paper "Art 28(2) USD: A harmonised BEREC cooperation process – Guidance paper" (BoR (13) 37), where the following practical issues were identified:

    - Fraud & misuse of numbers have an adverse impact on the confidence of end-users;
    - relating to the implementation of 28(2), identifying the forms of fraud, such as auto-dialling, short-stopping, PBX hacking, Wangiri calls etc.;

42. Relevant Authorities differ as in some Member States cases of fraud are referred to the NRA first, whilst in other Member States cases of fraud are referred to the judicial authorities The BEREC report on a review of the cross-border regulatory cooperation process within the scope of Art 28(2) USD (BoR (16) 226) reported that:

    - the process is used infrequently;
    - 4 NRAs initiated the process;
    - 3 NRAs responded to requests for assistance.

43. The speaker concluded noting that from the operators' side:

    - The perception of the scale of the issues varies;
    - Issues of confidentiality are often raised when providing information to NRAs;
    - Transit operators are not interested in prosecuting fraud as they are perceived to be time consuming.

6. Insights to fraud & misuse of numbers, a suggested role for NRAs - EETT

44. The final guest speaker, EETT's representative, shared views in respect to the issues in the Greek market and provided some general insights on fraud and misuse of numbers.

45. As noted by operators, NRAs are not acting in an efficient manner when it comes to fraud and misuse cases. On the basis of the answers to the relevant questions within the review of the International Roaming Regulation, it seems that NRAs do not expect a significant support from operators in resolving such cases.

[18] BEREC report on cross-border issues under Article 28(2) USD

46. The speaker believes that NRAs may be inadvertently contributing to the aforementioned issues because:

    1) They have extremely slow response times due to existing procedures and non-automated ways of exchanging information between the involved parties,

    2) They usually act in a reactive manner as they tend to respond to cases reported by the operators,

    3) For consideration - EU number database containing per country allocated type of number ranges (e.g. +3162 is mobile range in NL), link to where the national database with the individual allocated numbers can be found and which wholesale tariff scheme applies

    5) There is dispersed information among different entities about the issue (e.g. NRAs, EC, BEREC groups, ITU, Europol, Operators, GSMA, Interconnection Carriers) and

    6) They do not have jurisdiction on the Interconnection Carriers.

47. The Greek operators explained to EETT that it would be of extremely significant importance in dealing with fraud and misuse cases the possibility of having access to a shared database which contained the legally allocated numbering ranges per country (and per operator), including the PRS number ranges. Also, they asked to have access to a database of fraud and misuse cases per country through a system where all the operators are informed of the cases appearing in other countries and perhaps, for the NRA to act as a liaison between operators and Police/Europol.

48. The speaker suggested as a way forward for dealing with issues of fraud and misuse the set-up of a dedicated BEREC group that could be involved in collecting information about specific issues, reviewing guidelines periodically, consulting with stakeholders, perhaps helping in raising awareness among end-users, acting as a reference point for all NRAs and facilitating all NRAs to get a minimum level of understanding.

7. Panel discussion & Next steps

49. The panel discussion focused on how cooperation between NRAs can be improved and how NRAs and the outside organisations such as Europol can assist each other in the management and enforcement of powers where necessary to minimise the fraud and misuse of the numbers.

50. It was agreed that the “End-user” working group is not the correct work stream for dealing with “The fraud and misuse E.164 number range”, and therefore it was suggested that an alternative BEREC Working Group should be established in order to deal with this issue. Following the workshop, a discussion was held within BEREC and it was agreed that a work stream would be created to address the issue of the access to a common EU number database that stores details of numbers for cross checking purposes.

51. In addition, it was also proposed the establishment of a new task force that could address other issues like:

a. Slow inter-NRA response times.

b. Lack of automation when exchanging information.

c. Lack of access to the technologies used by those who perpetrated fraud and misuse.

d. The agreement of a common BEREC position on the description of what are cases of fraud and misuse.

e. Unification of the aims and methods of the various agencies and their approaches to the issues (e.g. NRAs, EC, BEREC groups, ITU, Europol, Operators, GSMA, Interconnection Carriers).

52. Another proposal was the establishment of a network of stakeholder in order to create a matrix of competent authorities and contact points with responsibility for Article 28(2) of the Universal Service Directive across Member States.

Annex 1

Q5 Please indicate whether your NRA deals with the following actions in relation to fraud and misuse:

Question 5	Yes	No
Approving a procedure to block, on a case-by case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues (Article 28.2 of the Universal Service Directive) stop payments to international carriers and ultimately the third party carrying out the fraud or misuse	BIPT, BNETZA, MCA, NKOM, NMHH, SPRK, OFCOM	AGCOM, AKOS, ARCEP, CNMC, COMREG, EETT, RRT, TRAFICOM
Resolving disputes between operators regarding fraud or misuse (Articles 20 and 21 of the Framework Directive).	AGCOM, AKOS, CNMC, MCA, NMHH, OFCOM, SPRK,	ARCEP, BIPT, COMREG, EETT, NKOM, RRT, TRAFICOM

BIPT *– It may on a considered case by case basis demand that operators block access to numbers and service when justified by the evidence. Generally, number holders comply with these requests when asked. (Article 51, § 5, of the Act of 13 June 2005 on electronic communications)*

BNETZA *– Will order deactivation if necessary (section 67(1) sentence 5 Telecommunications Act (TKG)). Orders to withhold relevant interconnection or other service revenues especially in cases of PBX/Router Hacking.*

MCA *– While national legislation stipulates that the MCA may require undertakings providing public communications networks and, or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reasons of fraud or misuse and to require that in such cases providers of electronic communications services withhold relevant interconnection or other service revenues, however, to date the MCA did not encounter situations where it required undertakings to block access to numbers/services and/or to withhold interconnection or other service revenues.*

NKOM – *Within National law (The Electronic Communications Act Section 4-2 a) there are regulatory provisions that have not yet been used. In the Ecom Regulations Section 6-1 there are also provisions for providers to block. Nkom has also encouraged providers to block on a case-by-case basis to prevent end-users from loss, this is based on private law.*

Nkom is currently in dialogue with providers concerning filtering/blocking based on call pattern analysis.

***NMHH** – The NRA has this competence only for premium rate numbers. The decisions so far have been issued as preliminary decisions to prevent further fraud and harm.*

***OFCOM** – Ofcom has published 'Enforcement guidelines for regulatory investigations' which explain in Section 8 the procedures that Ofcom will usually follow. Where Ofcom has reasonable grounds to suspect that fraud or misuse is occurring in connection with the use of a number or service, and that this conduct has caused or has the potential to cause consumer harm, we will consider whether it may be appropriate and proportionate to issue a direction under the UK's General Conditions. The direction would require providers to block access to that number and/or service and to withhold associated revenue.*

***SPRK** – According to NRA rules (Article 42 of General Authorisation Regulations in the field of electronic communications) electronic communication merchant to preclude fraud, using numbering or numbering misuse, can block number ranges or interconnection direction where fraud is detected or to prevent fraud attempt.*

Seven of the fourteen respondents answered "YES" to part "b" of question 5 and provided the following detail:

***AGCOM** – AGCOM, on request, resolves disputes between operators regarding fraud or misuse and AGCOM could suspend relevant interconnection or other service revenues. In case of reference offer of Telecom Italia cases of suspension are foreseen in deliberation no. 119/10/CIR. For example, a suspension of four months for the payments is allowed if Telecom Italia complains to the judicial authority.*

***AKOS** – Resolves disputes between operators, no matter what is the subject of the dispute.*

***CNMC** – The competence to resolve disputes between operators falls on these matters in the CNMC. The conflicts usually deal with withholding of payment for irregular traffic or the refund of any amounts. However, it is the Ministry (SEAD) the organization that has approved a procedure to block traffic and to withhold payment for irregular traffic under article 28.2 USD.*

***MCA-** The MCA have published guidelines for inter-operator complaints, disputes & own initiative investigations which are required to be followed. This publication is available at: https://www.mca.org.mt/articles/mca-guidelines-inter-operator-complaints-disputes-and-own-initiative-investigations-070111*

***NMHH**- Disputes are decided by a three-member panel appointed by the President of the NRA using a contradictory procedure. The procedure is conducted in writing but a hearing can be scheduled if necessary.*

***OFCOM** - Ofcom has published Dispute Resolution Guidelines - Ofcom's guidelines for the handling of regulatory disputes. Paragraphs 5.22 - 5.25 cover cross-border disputes.*

SPRK *- NRA deals with disputes between operators regarding fraud or misuse in accordance with law and rules as in other cases. Also SPRK defines a procedure and criteria to determine if specific case can be classified as fraud. The procedure and criteria are defined in the rules (now available only in Latvian). SPRK does not deal with any electronic communication merchants complains or disputes regarding payments. All such cases should be addressed in court.*

Q6 If not already done so, has your NRA implemented a process (since 2016) to deal with cases of fraud or misuse in order to:

Statement	Yes	No
prevent cases of fraud or misuse occurring;	**BNETZA, NMHH, OFCOM, SPRK**	**AGCOM, AKOS, ARCEP, BIPT, CNMC, COMREG, EETT, MCA, NKOM, RRT, TRAFICOM**
stop and minimize their impact on end-users;	**BIPT, BNETZA, COMREG, MCA, OFCOM, SPRK,**	**AGCOM, AKOS, ARCEP, CNMC, EETT, NKOM, RRT, TRAFICOM**
stop payments to international carriers and ultimately the third party carrying out the fraud or misuse.	**BNETZA, COMREG, OFCOM**	**AGCOM, AKOS, ARCEP, BIPT, CNMC, EETT, MCA, NKOM, RRT, SPRK, TRAFICOM**

If YES to any of the above, please provide details including any factors you may consider before taking on a case such as the financial thresholds for intervention, resources available etc.

AGCOM *– AGCOM has not implemented a process to deal with cases of fraud or misuse but the contrast to fraud and misuse is realised through a national committee established by AGCOM deliberation no. 418/07/CONS.*

BIPT *– BIPT provided a specific email address for operators to notify any suspicious behaviour regarding international phone calls (Wangiri-fraud). BIPT then transmits the details of the suspicious phone calls to the (network) operators for further investigation, without disclosing the identity of the notifying operator. When affected by the malicious phone calls, network operators are also requested to take appropriate measures the avoid consumer harm and to report back to BIPT. In 2019 it was agreed between BIPT and the operators that notifications of suspected phishing practices through SMS (smishing) could also be included in this notification process. In relation to misuses of premium rated numbers, see answer 5a.: the BIPT invites number holders to block access to these numbers, in order to prevent future harm.*

BNETZA *– Withholding interconnection or other service revenues at a domestic level.*

CNMC- *The competent body to dictate or approve the measures is the Ministry of Economy and Competition by Royal Decree 381/2015, of May 14, which establishes measures*

against illegal traffic and irregular traffic for fraudulent purposes in electronic communications. There are two kind of procedures:

A) The operator blocks and send a report to the Ministry afterwards: Before blocking, each operator must send an application form explaining the criteria that the traffic should meet to be considered fraudulent or irregular. Once these criteria have been approved by the Ministry, operator can block the traffic and withhold the payments. After that, he must notified this blocking to the Ministry in two days' time and the Ministry can check if the traffic meet the criteria approved for that operator.

B) The operator requires authorization from the Ministry before blocking fraudulent traffic: Once the fraudulent traffic has been detected, the operator that has not the procedure (explained in A) approved can ask the Ministry for a permit to block the traffic.

***MCA-** Following various occurrences of Wangiri scam calls worldwide which also affected subscribers in Malta, an information sharing process has been established during 2017 following an agreement between the MCA and all local telephony service providers. When a local telephony service provider blocks outgoing calls to an international number or number range after it is identified as being misused and/or fraudulently used, this information is shared with the MCA who in turn informs all local telephony service providers so that each service provider may then decide whether to block outgoing calls to the identified number or number range. The MCA does not divulge the identity of the telephony service provider providing this information due to confidentiality reasons.*

***NKOM –** Nkom is in dialogue (2018/2019) with the national police and providers, and there has been arranged workshops. However no formal process has been implemented.*

***NMHH**- Consider the number of impacted subscribers and operators and the damage incurred. Cases are dealt with by electronic communications surveillance staff as needed.*

***OFCOM** - Ofcom has launched a number of initiatives to help prevent cases of fraud and misuse, and to minimise their impact on end-users. These consist mainly of working collaboratively with industry and competent authorities, as follows:*

- *convening an industry Strategic Working Group of the 10 largest providers to share experiences and insights into fraud and misuse. This includes sharing blocked number information via Ofcom;*
- *working with financial and other relevant organisations to compile a 'Do Not Originate' list of numbers to be blocked from making outbound calls;*
- *identifying numbers that are the subject of consumer complaints or where call patterns associated with fraud and misuse are detected, analysing the data and providing the list of numbers to the Strategic Working Group for due diligence purposes;*
- *publishing a list of protected number blocks to help providers block calls from unassigned numbers;*
- *creating a new number range (08979) to be used as inserted Network Numbers when a call entering the UK has unreliable or untrusted CLI. This leads to a more efficient call tracing process in cases of fraud and misuse.*

Also see answer to Q5 re processes regarding enforcement and dispute resolution

SPRK *- NRA has defined a procedure, how electronic communication merchants and NRA deal with frauds and numbering misuse (Fraud, using numbering, prevention rules). The rules include: fraud criteria; process description how operators deals with fraud and informs SPRK about fraud; how SPRK deals with fraud application from operator, including terms and cooperation with Latvia and other countries competent authorities.*

It is up to the operators to stop the payments in case of fraud or numbering misuse but to pervert disputes and make operators conscious about the payments in case of frauds SPRK has included in the electronic communication law and in rules requirement that the interconnection contract shall provide the procedures by which call routing and access to numbers and electronic communications services is to be terminated, as well as the procedures for mutual payments in cases when fraud performed using numbering or incorrect use of numbering is detected.

Q7 If you answered Yes to Q6 above, does your process include cross border regulatory cooperation as recommended in BoR (13)37? YES ☐ NO ☐

a) If YES please provide the relevant details in accordance with the table included in the sheet titled "Q6" of the attached Excel spreadsheet.

Statement	Yes	No
Does your process include cross border regulatory cooperation as recommended in BoR (13)37	**COMREG, NMHH, OFCOM, SPRK,**	**AGCOM, BIPT, BNETZA, CNMC, EETT, MCA, RRT, TRAFICOM**

Q8 Are the financial thresholds indicated in BoR (13)37 for retail operators and transit operators set at a realistic and practical level? YES ☐ NO ☐

Statement	Yes	No
Are the financial thresholds indicated in BoR (13)37 for retail operators and transit operators set at a realistic and practical level	**AKOS, BNETZA, COMREG, NMHH,**	**BIPT, EETT, RRT**

BIPT *– Apart from the legal impossibility for the BIPT to autonomously qualify a practice as fraud (see above), the BIPT believes that executing Art. 28(2) USD is not very effective nor efficient to fight telecom fraud. This is due to the long procedural throughput time and the fact that it is almost impossible in practice to track and punish fraudsters. That is why the BIPT suggests a pragmatic approach (see e.g. question 6) to prevent and fight fraud. This approach exists in realizing an exchange of information and collaboration between the anti-fraud departments.*

BNETZA *– There are no fixed financial thresholds.*

MCA – *The MCA is not in a position to comment on this aspect since to date it did not receive any formal complaints or reports on cross-border misuse and/or fraudulent use of numbers requiring investigations.*

NKOM- *At this point Nkom cannot answer yes or no on this question since the efficiency of the process needs to be discussed first.*

NMHH*- The thresholds are realistic and usable as a guide*.

OFCOM- *Ofcom was part of the drafting team working on BoR (13)37. We gave significant thought to setting an appropriate threshold. We recognised that NRAs did not have the resource available to react to insignificant amounts, but on the other hand, if a very large number of end users experience the same fraud the total may become significant. We tried to balance these considerations when setting the thresholds. We have not experienced any difficulties with the levels set.*

TRAFICOM- *Information is not available. Should be enquired of operators*.

Q9 In reference to your answer to Q6, what other issues do you consider when initiating a case under this process?

BIPT *– See answer to Question 8.*

BNETZA *– Ban on billing and collecting charges addressed to originating network operator.*

MCA *– Not applicable, the process described in the response to Question 6 was established solely for information sharing purposes among local telephony service providers.*

NMHH *– Number of affected subscribers and operators, nature of incident, amount of damage.*

OFCOM *– Relevant issues include:*

- *Timescales, including how recently the experience of fraud/misuse occurred. Is the revenue likely to have been paid to the perpetrator already? Are we able to obtain the relevant CDRs to pursue call tracing?*
- *Financial thresholds*
- *Number of complaints re the numbers in question*
- *Whether the fraud was targeted at vulnerable and/or older consumers*
- *Any other issues that might contribute to the serious of the case and the likelihood of resolving the case*

SPRK *– Latvia and other countries competent authority's responses if there are required by SPRK.*

TRAFICOM – *Competent authority should be decided, an usable process should be created and thresholds when to start process. The most important is now and how fast operators react.*

Q 10 Are you aware of any measures being taken independently by operators in your jurisdiction to address and mitigate cases of fraud or misuse? Yes /No

If YES, please advise on any measures being taken

Statement	Yes	No
Are you aware of any measures being taken independently by operators in your jurisdiction to address and mitigate cases of fraud or misuse	**AGCOM, AKOS, BNETZA, CNMC, EETT, NKOM, NMHH, OFCOM, RRT, SPRK, TRAFICOM**	**BIPT, COMREG, MCA**

AGCOM *– Sharing of information within the national committee, concerning also the evolution of the number of fraud and misuse.*

AKOS *– Operators are publishing numbers for which they assume that are abused.*

BNETZA *– Fraud detection, withholding payments/interconnection fees in case of fraud/misuse.*

CNMC- *Block traffic, (ii) stop interconnection payments, and (iii) including in the interconnection agreements provisions about stopping traffics when there is fraud or misuse involved, and also retaining payments in those cases.*

COMREG *- ComReg's decision to intervene is based on the following factors: case has been registered with the Gardaí, relevant information has been provided in sufficient time, the operator will not charge the end-user for the calls and wholesale costs for the relevant calls are at least €5000. ComReg may not intervene in cases where it is a repeat incident or where the end-user is an authorised operator.*

EETT- *Most of the Operators have deployed anti-fraud software systems and have established relevant policies and procedures in order to mitigate fraud cases.*

NKOM- *Operators block thousands of calls on a daily basis, and is currently in a dialogue with Nkom on filtering measures. An expert group has been formed to address issues, specifically with regards to spoofing.*

NMHH*- Number of affected subscribers and operators, nature of incident, amount of damage.*

OFCOM *– Operators have their own measures to identify, react to and reduce incidences of fraud and misuse. These include monitoring call patterns to identify those that might be associated with inappropriate use (for example short duration calls, significant levels of call origination from a number) and responding to complaints and shared industry information on suspicious calls. Operators then investigate and compile their own blocked number lists, as well as respond to Ofcom and industry intelligence. Also see answer to Q6.*

RRT *– Operators have their own tools how to react to identify cases of frauds for protection its services and subscribers. For example, operators can block incoming calls*.

SPRK *– Fraud detection systems; defining in the agreements fraud and the measures that should be taken in case of fraud or numbering misuse; intervention with the police regarding happened fraud cases; interaction with SPRK, other competent authorities and related merchants in case of fraud to define if the case meet fraud criteria and to inform others about the threat.*

TRAFICOM *– Some operators have blocked certain numbers to prevent Wangiri-calls. Might be other measures too, but they are not reported to the NRA.*

Q11 Has your NRA cooperated with other NRAs in cases of cross border fraud or misuse? YES/NO

If YES please provide the relevant details in accordance with the table included in the sheet titled "Q11" of the attached Excel spreadsheet.

Q11	Yes	No
Has your NRA cooperated with other NRAs in cases of cross border fraud or misuse	**BNETZA, EETT, NMHH, OFCOM, SPRK,**	**AGCOM, AKOS, ARCEP, BIPT, CNMC, COMREG, MCA, NKOM, RRT, TRAFICOM**

OFCOM- *Yes, from time to time we have responded to other NRAs' requests however not in terms of being able to answer the questions in the Q11 spreadsheet. We have been notified of investigations by NRAs (most commonly ComReg) without any request for our action. We have also been asked to cooperate with some NRAs but not able to do so. For instance, we received a request from the Latvian NRA in October 2018. However, we were unable to help with information sharing as the incident had happened too long ago and UK operators would not hold the necessary CRDs to trace the call and be able to help in the Latvian NRA's investigation.*

Q12 Has your NRA utilized the provisions of Article 28(2) USD to block access to numbers or services and in such cases required providers of electronic communications services to withhold interconnection or other service revenues <u>at a domestic level i.e. within your Member State without having to engage in cross border co-operation</u> YES/NO

If YES please provide the relevant details in the table included in the sheet titled "Q12" of the attached Excel spreadsheet, having regard for the details in Column E related to any cross border aspects to these cases.

Q12	Yes	No
Has your NRA utilized **the provisions of Article 28(2) USD to block access to numbers or services and in such cases required providers of electronic communications services to withhold interconnection or other service revenues <u>at a domestic level</u>**	**AGCOM, BNETZA, CNMC, COMREG, NMHH, OFCOM**	**AKOS, ARCEP, BIPT, EETT, MCA, NKOM, RRT, SPRK, TRAFICOM**

OFCOM- *A direction was issued by Ofcom in May 2016 instructing certain UK providers to block access to a list of UK 08 chargeable non-geographic numbers due to nuisance call incidents. Do not have the relevant details available to complete the Excel spreadsheet.*

Q13 In general, irrespective of whether or not local operators manage to stop interconnection payments, what is the common practice regarding charging end-users for fraudulent/misuse calls?

AGCOM *– If the end-user complains a charging for fraudulent/misuse calls the common practice is that such calls are not charged by the operator.*

AKOS *– Article 146 of Electronic Communications Act, paragraph 2 stipulates: "In instances of abuse committed by third persons and not arising due to subscribers or user fault, public communications service providers shall accept the costs incurred as a consequence of the abuse." AKOS therefore would grant end-users that they do not have to pay the costs incurred due to the reported abuses.*

ARCEP *– Some operators ask end-users to pay for a small fraction of the amount charged and others charge nothing.*

BIPT – *We have no specific information on this topic. It probably depends on the case and the operator involved whether the amounts charged are credited yes or no by way of a "commercial gesture".*

BNETZA *– Ban on billing and collecting and payment ban addressed to network operators/"bill issuer".*

CNMC *– The majority of the cases examined by CNMC involve operators only. However, when there are end users, the common practice is to return them the amount paid and retained by the operator.*

COMREG *– Where ComReg makes a decision not to intervene in case, the Operators usually only charge the end user the wholesale value of the calls. Where ComReg makes a decision to intervene in a case, Operators do not charge the end users for the fraudulent calls.*

NKOM *– Varying on the type of fraud, the amount of money, time passed since the incident, documentation from local police, and interconnection agreements.*

NMHH *– Depending on the operator and the amount of damage as well as the impacted subscribers, operators may waive the charges stemming from fraud. Especially smaller operators cannot afford this, however.*

MCA *– The MCA does not have such information in hand.*

RRT *– Usually payment is not charged from end-user.*

SPRK *– Usually operators do not charge any fee. Fee is charged in the case, when fraud happened on end-user fault.*

TRAFICOM *– Unknown, but we know that there have been instances of where calls have not been charged when the issue affected a larger number of consumers.*
According to Information Society Code Section 337
Closing a number or service
The Consumer Ombudsman may under penalty of a fine order a telecommunications operator to close a number or otherwise bar the use of a service

if it is evident that the service seeks unlawful financial benefit by providing information in marketing material that is essentially false or misleading with regard to subscribers and users, and if fees resulting from the service accumulate on the subscriber's communications service bill. The Consumer Ombudsman may also issue a temporary decision, which remains in force until a final decision has been reached in the case.
Operators have been under more pressure to monitor and stop such cases as due to legislation introduced in 2015, operators are in joint liability with service providers whose services they charge. According to Section 128(1) of the Information Society Code, "A consumer who has the right to refrain from paying, or receive a refund, compensation or other payment from a business operator due to the operator's breach of contract shall have the same right in relation to the telecommunications operator that has charged the consumer for a commodity.

Q14 Has your NRA found any cases of fraud or misuse not previously identified in Section 3.2.2 of BoR (13) 37? YES/NO

If YES please provide the relevant details in accordance with the table included in the sheet titled "Q14" of the attached Excel spreadsheet.

Q14	Yes	No
Has your NRA found any cases of fraud or misuse not previously identified in Section 3.2.2 of BoR (13) 37	**AGCOM**	**ARCEP, AKOS, BNETZA, CNMC, COMREG, EETT, MCA, NMHH, OFCOM, RRT, SPRK,**

AGCOM *– CLI spoofing. CLI of non-EU countries is switched to numbers of the EU numbering plan so that termination rate for call originated in EU is applied.*

BIPT *– The cases of fraud have already been sufficiently documented (see among other things the recent report of 30 May 2018 "The role of E.164 numbers in international fraud and or misuse of electronic communications services" of the CEPT ECC: https://www.ecodocdb.dk/download/e2070f50-a63b/ECCRep275.pdf)*

NKOM *– Nkom agrees with the statement from BIPT: „The cases of fraud have already been sufficiently documented (see among other things the recent report of 30 May 2018 "The role of E.164 numbers in international fraud and or misuse of electronic communications services" of the CEPT ECC: https://www.ecodocdb.dk/download/e2070f50-a63b/ECCRep275.pdf)"*

TRAFICOM *– SIM-box cases: calls from abroad are routed through illegal SIM-box to avoid roaming costs.*
- Smishing cases: Name of the SMS sender is spoofed.
- Wangiri-calls: A-number spoofing, and telephone stealing and calling to expensive numbers.

Q15 Do you consider that more needs to be done to promote the benefits of using BEREC Guidelines and facilitating cooperation YES/NO

If YES please provide the relevant details in accordance with the table included in the sheet titled "Q11" of the attached Excel spreadsheet.

Q15	*Yes*	*No*
Do you consider that more needs to be done to promote the benefits of using BEREC Guidelines and facilitating cooperation	**AGCOM, BNETZA, CNMC, COMREG, EETT, NKOM, NMHH, OFCOM, RTR, SPRK**	**AKOS, TRAFICOM**

AGCOM *– BEREC guidelines could be reviewed also taking into account the topics dealt with in questions 16 and 17.*

BNETZA *– Contribute to the improvement of processes*

CNMC *– BEREC should send a communication given information about the existent procedure, the contact person at BEREC and asking the different NRA about the contact person in cases of fraud or misuse in the specific NRA and the department in charge.*

COMREG *– NRA contact network (updated list). High Level listing of NRA competencies in the area of Fraud and/ misuse.*

EETT *– Taking into consideration the evolution and increase of misuse/fraud telecom cases we should consider the setting up of a BEREC dedicated group that would be involved in collecting information about the issues, reviewing any guidelines periodically, consulting with the stakeholders (EC, telecom NRAs, Europol, cybercrime units, interconnection carriers, providers, authorities responsible for personal data and privacy, ENISA, consumer associations) and disseminating relevant information to the NRAs.*

NKOM *– The promotion of guidelines should be considered after discussing the efficiency of the current guidelines.*

NMHH *– The visibility of the guidelines should be increased along with operators' awareness of the procedures.*

OFCOM *– Co-operation and sharing of information and expertise are vital to combating fraud and misuse. NRAs need to work together, and with industry and relevant competent authorities. BEREC should also work collaboratively with the relevant numbering experts in CEPT/ECC. Within the ECC, the Working Group Numbering and Networks (WG NaN) is working on measures to restore trust in numbers, including work on fraud and misuse (see reference to CEPT workshop held in December 2018 in the introduction to this questionnaire). WG NaN is considering ways to extend the BEREC cooperation process to all 48 CEPT countries.*
Section 6 of the BEREC internal report made a number of conclusions and recommendations on improving the effectiveness of the cooperation process. It is not clear that these have been progressed. They should therefore form the starting point for reviewing the cooperation process and promoting its benefits.

SPRK *– Hold workshops in purpose to discuss the latest information and cases regarding fraud and numbering misuse. To have a database of contacts of institutions and people, which can be contacted in case of cross border fraud and numbering misuse.*

Q16 Do you consider that a common database of contact points for each NRA or relevant authority would assist in cooperation among member states on the issue of fraud and misuse YES/NO

If YES please provide the relevant details

Q16	Yes	No
Do you consider that a common database of contact points for each NRA or relevant authority would assist in cooperation among member states on the issue of fraud and misuse	**AGCOM, AKOS, BNETZA, CNMC, COMREG, EETT, MCA, NKOM, NMHH, RRT, SPRK, TRAFICOM**	**TRAFICOM**

BNETZA *– Facilitates contact in cross-border cases*

COMREG *– This would help more positive engagement and open conversations around the fraud and misuse.*

EETT *– Perhaps it could be of help, according to the review of the existing procedure*

NKOM *– However, fraud cases are mostly non-European. ITU could be a holder of such a database.*

NMHH *– Having a list of contact points makes it easier and faster to make contact.*

OFCOM *– This was always the intention behind the process, to be administered by the BEREC Office. As fast reactions to requests for information are vital, it is important that relevant contacts are easy to identify and that the contact person knows the process and is ready to react.*

SPRK *– That would make faster the investigation of frauds and numbering misuse.*

TRAFICOM *– Who would give the data to whom, who would be the contact point? Operators don't have to report to NRA so visibility is not good.*

Q17 Do you consider that a reference database with a register of cases of fraud or misuse reported by NRAs in each country would act as a knowledge base for NRAs and would facilitate the review of trends and the effectiveness of the processes being undertaken? YES/NO

Q17 -	Yes	No
Do you consider that a reference database with a register of cases of fraud or misuse reported by NRAs in each country would act as a knowledge base for NRAs and would facilitate the review of trends and the effectiveness of the processes being undertaken	AGCOM, AKOS, BNETZA, CNMC, COMREG, NKOM, NMHH, OFCOM, RRT, SPRK, TRAFICOM	BIPT, EETT, MCA

BIPT *– The cases of fraud have already been sufficiently documented (see among other things the report entitled "The role of E.164 numbers in international fraud and or misuse of electronic communications services" of the CEPT ECC: https://www.ecodocdb.dk/download/e2070f50-a63b/ECCRep275.pdf). It is useful, however, to organise basic workshops with the industry on a regular basis (see e.g. the public workshop on the role of E.164 number in international fraud and misuse of electronic communication services – Brussels, 11 December 2018) https://www.cept.org/ecc/groups/ecc/wg-nan/news/public-workshop-on-the-role-of-e164-numbers-in-international-fraud-and-misuse-of-electronic-communications-services-brussels-11-december-2018/*

BNETZA *– Because of diverging national competences and toolsets we see only limited added value in such a database. Proper cooperation mechanisms would be more useful*

COMREG *– A reference database of cases could help spot patterns of where the traffic is coming from and help to assist operators in protecting their customers. However it could become very big and cumbersome sand so would need a good search facility.*

EETT *– Not all cases are being submitted to the NRAs. In the context of reviewing the procedures we need find in collaboration with other stakeholders any relevant measures to prevent fraud and misuse.*

MCA *– Since this could be substantial the MCA believes that a Member State would be in a position to check directly with the other Member State in question*

NMHH *– It is useful to observe trends, but may also be used to track serial offenders and entities operating in more than one member state*

OFCOM *– Sharing of information and cases as reference tools and to spot trends should be beneficial.*

SPRK *– Yes, but each NRA may have an additional cost to update the information into the database. Also, the access to database should be restricted.*

TRAFICOM *– Might be helpful if cases are in statistical mode and anonymous.*

Q18 Do you consider it necessary to publish the;

Statement	Yes	No
Numbers that have been blocked or to include them in a database?	AKOS, BNETZA, CNMC, NMHH, RRT, SPRK, TRAFICOM	BIPT, COMREG, EETT, MCA, NKOM, OFCOM
the name of the operators that committed fraud or misuse	AKOS, BNETZA, CNMC, NMHH, RRT, SPRK, TRAFICOM	BIPT,COMREG, EETT, NKOM, OFCOM, MCA
If YES, Do you deem it necessary to create a template with the necessary information?	AKOS, CNMC, OFCOM, RRT, SPRK, TRAFICOM	BIPT, BNETZA,EETT, NKOM, NMHH

AKOS – *It would be more transparent.*

BIPT *– It is useful, however, to organise basic workshops with the industry on a regular basis (see e.g. the public workshop on the role of E.164 number in international fraud and misuse of electronic communication services – Brussels, 11 December 2018).*

BNETZA *– BNetzA publishes all measures and involved numbers (www.bundesnetzagentur.de/Massnahmenliste), names only a case by case basis.*

COMREG *– It is very difficult to find the source of the fraud or misuse and may not be directly linked to an operator, so publishing their names would not be useful.*

EETT *– Taking into consideration the evolution and increase of misuse/fraud telecom cases we should consider the setting up of a BEREC dedicated group that would be involved in collecting information about the issues, reviewing any guidelines periodically, consulting with the stakeholders (EC, telecom NRAs, Europol, cybercrime units, interconnection carriers, providers, authorities responsible for personal data and privacy, ENISA, consumer associations) and disseminating relevant information to the NRAs.*

MCA – *In extreme circumstances Member States would be in a position to inform all other Member States for particular numbers through the database of contact points on a case by case basis.*

NMHH *– A template may make it easier to provide complete information.*

OFCOM *– It is not 'necessary' to publish this information for two or more NRAs to cooperate on a case of fraud or misuse. Publishing such information would require a number of caveats to be satisfied and evidence thresholds to be met. Also, administration of any such list would need to be kept 'up-to-date' as number blocking can be time-limited.*

Templates should serve to streamline the process but must not be too prescriptive, as this might causes delays and discourage use of the cooperation process.

SPRK *– Information about transit operators should also be included into database. The template would fasten the data update process. Access to database should be restricted*

TRAFICOM *– It would be important to identify repeated fraud cases and operators involved to those. Competent NRAs could do measures result of fraud.*

Q19 Do you consider that some best practice guidelines, such as those noted below, would help to reduce the number of fraud and misuse cases in the future and to assist you in dealing with such cases?

Statement	Yes	No
Contract clauses facilitating the withholding of revenue	**AGCOM, AKOS, BIPT, BNETZA, COMREG, EETT, NKOM, MCA, NMHH, OFCOM, RRT, SPRK, TRAFICOM**	
Raising standards in end-user protection	**AGCOM, AKOS, BNETZA, COMREG, EETT, MCA, NKOM, NMHH, OFCOM, RRT, SPRK, TRAFICOM**	**BIPT**
Cooperation with police and other enforcement and regulatory agencies.	**AGCOM, AKOS, BIPT, CMNC, COMREG, EETT, MCA, NKOM, OFCOM, RRT, SPRK, TRAFICOM**	**BNETZA, NMHH**

AKOS – *Not necessary, but welcome*

BIPT *– Quickly stopping the cash flow is of crucial importance. When necessary, police and other enforcement and regulatory agencies have to cooperate but this is a matter for the back office. Consumers need one unique point of contact to file their complaint.*

BNETZA *– Helpful to improve the situation.*

EETT *– It is important to blocking the flow of money and have a close cooperation with Europol and other stakeholders.*

TRAFICOM *– Operators can decide if they want to use standardized contract clauses...*

Q20 Blocking numbers:

a) what are the most common numbering ranges blocked

AKOS - *AKOS does not have a record of blocked numbers, because they can be blocked only by Court order. Operators do not block numbers where abuses are detected, but calls are charged at the highest price.*

BIPT *– Premium rated numbers.*

BNETZA *– Constantly changing.*

CNMC *– In disputes related with fraud and misuse, CNMC usually deals with special rate numbers, directory numbers (118) and 902 (non-geographical intelligent network numbers- they are usually used for customer services and they do not have regulated termination rates.).*

COMREG *– Carried out by Operators.*

MCA *– The number ranges which are being blocked are typically those used for Wangiri scam calls.*

NKOM *– Ranges related to high cost destinations.*

NMHH *– In Hungary only inland premium numbers may be blocked by the NRA*

OFCOM *– All number types may feature on our number blocking list. The most common at the moment at 03 numbers. These are non-geographic numbers charged at a geographic rate (they are included in relevant call allowance packages and are a relatively low call cost where not included). The reason these numbers are on the list currently is that they are linked with a CLI spoofing scam on a Government Revenue and Customs helpline.*

RRT *– Operators do not provide such information.*

SPRK *– No information*

TRAFICOM *– Numbers which are used in Wangiri-frauds, satellite numbers. Also numbers used in SIM-boxes are blocked. GSMA-and other fraud lists.*

b) Once the block procedure is set in motion, for how long do these numbers remain blocked

BIPT *– Until they are reassigned, at the operator's convenience.*

BNETZA *– At least 1 year partially permanent.*

CNMC *– 1 year.*

COMREG *– Carried out by Operators.*

MCA *– No timeframe is set however the MCA requires undertakings to inform it when numbers/number ranges are unblocked.*

NMHH *– If blocking was preliminary, then until the conclusion of the investigation, otherwise until the fraud / misuse has been stopped.*

OFCOM *– Some numbers will not be unblocked, e.g. those numbers not used to originate calls legitimately. Others may be time-limited on a case-by-case basis.*

RRT *– Operators do not provide such information.*

SPRK *– No information. It is not specified in Latvia legal acts. Also, the problem with number ranges being blocked by GSMA, where SPRK and fixed operators do not have access to the information, arises.*

TRAFICOM *– According to the Act on Electronic Communications Services (917/2014) section 272 measures taken to implement information security (such as blocking) must be discontinued if the conditions for them specified in this section no longer exist.*

Q21 Does your procedure for blocking numbers apply to wholesale, retail or both?

Q21a	Yes	No	Both
Does your procedure for blocking numbers apply to wholesale, retail or both?		**ARCEP, BIPT, BNETZA, COMREG, EETT,**	**ARCEP, CNMC, NKOM, OFCOM, SPRK**

Does the procedure vary depending on whether it occurs at the wholesale or retail level? If YES, can you describe the differencesYES/NO

Q21b	Yes	No	Both
Does the procedure vary depending on whether it occurs at the wholesale or retail level?		**BIPT, CNMC, COMREG, NMHH, SPRK,**	**BNETZA, NKOM, NMHH, OFCOM**

AKOS – *Numbers can be blocked only by Court order.*

BNETZA *– When it has reliable information about the unlawful use of a number the Bundesnetzagentur will typically order deactivation/disconnection of the number. The addressee is always the network operator in whose network the number is set up. Deactivation/disconnection makes sure that the numbers are no longer available and that no charges are payable for connection to them.*

CNMC *– The blocking is always taken by operators at wholesale level when the traffic fulfil some parameters but the victim can be operators or end users.*

MCA *– Once a local telephony service provider receives information as part of the process described in the response to Question 6, it may decide whether to block outgoing calls to the identified number or number range and, if yes, whether outgoing calls to these numbers would be blocked solely for calls originating from its retail subscribers and/or also for wholesale traffic (e.g. inbound roaming traffic, transit traffic, etc.).*

RRT *– NRA does not regulate produce for blocking numbers.*