



Europe

**GSMA Europe Response to the BEREC  
Public Consultation on**

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

16 November 2012

**Martin Whitehead**  
**Director GSMA Europe**

Park View, 4th floor  
Chaussée d'Etterbeek 180  
1040 Brussels  
E-mail: [mwhitehead@gsm.org](mailto:mwhitehead@gsm.org)  
[www.gsmeurope.org](http://www.gsmeurope.org)

**Register ID Number: 30988577529-37**

## About the GSMA

The GSMA represents the interests of mobile operators worldwide. Spanning more than 220 countries, the GSMA unites nearly 800 of the world's mobile operators with more than 230 companies in the broader mobile ecosystem, including handset makers, software companies, equipment providers and Internet companies, as well as organisations in industry sectors such as financial services, healthcare, media, transport and utilities. The GSMA also produces industry-leading events such as the Mobile World Congress and Mobile Asia Expo.

For more information, please visit the GSMA corporate website at [www.gsma.com](http://www.gsma.com) or Mobile World Live, the online portal for the mobile communications industry, at [www.mobileworldlive.com](http://www.mobileworldlive.com)

---

In the European Union the GSMA represents over 100 operators providing more than 600 million subscriber connections across the region.

[www.gsmworld.com/gsma\\_europe](http://www.gsmworld.com/gsma_europe)

## **1 Introduction**

- 1 The GSMA welcomes the opportunity to submit its views on BEREC's draft report on Article 28(2) Universal Service Directive and the harmonised BEREC cooperation process. The GSMA shares the BEREC objectives of providing consumers with the widest possible access to services across Member States while simultaneously increasing consumer protection and tackling fraud and misuse.
- 2 As the GSMA is a global association that represents the interests of more than 800 operators and more than 230 entities in the broader mobile ecosystems, including transit carriers, we have provided a general response reflecting the views of the GSMA's members. The structure of the response is based on the questions posed in BEREC's draft report, and additional general comments and suggestions are provided at the end.
- 3 Leadership within the GSMA on fraud and misuse issues is provided by the Fraud Forum (FF) working group, a global forum for developing and exchanging fraud management intelligence and best practice for mobile network operators. Independently of this consultation, FF views on tackling fraud and misuse were shared with BEREC through the participation by FF representatives at BEREC's fraud and security workshop in Lemesos, Cyprus on September 26<sup>th</sup>.

## **2 Executive Summary**

- 4 The GSMA welcomes any initiative that aims to minimise the impact of fraud on consumers and operators and disrupt the financial gain to a perpetrator of fraud or misuse. The GSMA also welcomes the leadership role that BEREC is taking to address the problem of fraud and misuse within the European Union. As a global organisation, the GSMA would hope that a practical and effective solution can be developed within the EU and ultimately be extended to other regions and jurisdictions.
- 5 The consultation process is sincerely welcomed by the industry. Given the significant role that operators and transit carriers will play in execution of the proposed BEREC process, the GSMA believes that additional follow-up consultation between GSMA members and BEREC would be mutually beneficial. This will ensure that any process to be implemented has the support and confidence of participating stakeholders from within the GSMA membership.
- 6 The proposals in the consultation paper have stimulated a range of feedback from GSMA members, but the general consensus is one of support for the aims of the paper. Further work is required to improve the proposed BEREC process so that it can be efficient and effective. The GSMA is eager to collaborate with BEREC to achieve this objective.
- 7 BEREC states there are three main objectives of the process:
  - to protect the interests of consumers
  - to protect the interests of operators
  - to prevent perpetrators of fraud or misuse from benefitting from their behaviour

These objectives are achievable. However, the process proposed by BEREC needs development and amendment to maximise the likelihood of success. Payment withholding is a powerful tool in the fight against fraud and misuse, but it must be used appropriately. NRAs must avoid the risk of undermining confidence in the international interconnect framework and triggering commercial disputes as a result of the payment withholding element of the process. Such disputes could ultimately lead to the cancellation of interconnect contracts between operators and transit carriers, potentially reducing competition and access to services by consumers and increasing costs.

## **2.1 Summary of Process Comments**

- 8 The proposed process would be more effective if it is kept as simple as possible and is optimised for rapid execution. More detail is needed and should include the service level expectations that will be needed between NRAs, operators, transit carriers, police and the BEREC office in order to execute the process efficiently and effectively.
- 9 The paper concentrates on designing a process centred around a legitimate end user. Although the GSMA recognises the important need to protect consumers, it should be noted that in many cases of organised fraud and misuse, a dishonest end user acquires service fraudulently with the intention of abusing operator services in order to artificially inflate traffic and dishonestly generate revenue. Alternatively, organised criminals gain access to the telephony services of legitimate end users (e.g. through phone theft, account takeover or PBX hacking) and exploit them for the same objective. The proposed BEREC process should disrupt end users who fraudulently generate calls on operator networks while also protecting legitimate end users, who may suffer from the consequences of fraud.
- 10 Numbering resource misuses such as short-stopping, number range hijacking and the abuse of unallocated numbers are often involved fraud incidents. In such incidents, a series of requests must be initiated under the proposed process by the originating NRA to determine the true routing of the call. This information gathering phase will delay any payment withholding action at the terminating end of the call, which benefits the perpetrators of fraud and misuse.
- 11 It is the GSMA Fraud Forum's experience that fraudsters adapt their methods when new mechanisms are introduced to disrupt their activities, and that they will find and exploit vulnerabilities in a business process or fraud control mechanism. The proposed process is open to exploitation, as follows:
  - Potentially inconsistent application of process across NRAs. Fraudsters will adapt their activities to exploit communications services available in Member States where experience shows that NRAs intervention is least likely or has proven to be least effective.
  - Inability of process to compel action outside of EU Member States. As illustrated in the proposed BEREC process, the communications traffic chain includes multiple operators and transit carriers. In today's global interconnect environment, perpetrators of fraud and misuse can quickly adapt their methods to ensure that at least one leg of the traffic chain is routed via a

country outside of the EU without a similar ability to intervene. This significantly undermines the process.

- It is likely that fraudsters will be able to continue to operate profitably below thresholds without fear of intervention by perpetrating an increased number of fraud incidents with a lower associated value per incident.

There is a risk that current fraud and misuse methods may adapt to focus on these vulnerabilities, reducing the effectiveness of the proposed BEREC process.

- 12 The GSMA is eager to work with the BEREC Expert Working Group (EWG) to develop a solution to fraud and misuse and looks forward to further engagement on this topic. With this in mind, the GSMA extends an open invitation to BEREC EWG members to join a GSMA Fraud Forum meeting during 2013 – contact [ff@gsm.org](mailto:ff@gsm.org) for details.

## 2.2 Other Suggestions

- 13 The GSMA believes that numbering resource misuse is a key enabler for fraud. NRAs can help to address the issue of numbering resource misuse independently of the proposed BEREC process through stricter national number range management, e.g.
- Maintenance and publication of comprehensive and accurate national numbering plans.
  - Application of stricter controls over the assignment of number ranges and monitoring of their use
  - Implementation of controls over leasing of number ranges by number range assignees to third parties.

## 3 Responses to Specific Questions in BEREC Consultation Paper

### 3.1 *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.*

#### 3.1.1 Service Availability and Fraud Management

- 14 Section 2.4, paragraph 27 of the document states “*At the retail level it is important to ensure that operators put in place efficient systems and processes to detect and handle fraud and ensure sufficient end-user protection.*” There is little incentive for an operator to do this for retail traffic originated on their network if they have a route through which they can block onward payment to their carrier. In fact, if 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.
- 15 The existence of a payment withholding process for fraudulent traffic which reduces the risk to retail operators may give them an incentive to offer greater access to services to end users. In the absence of such a process, high-value and/or high-risk services might only have been available to customers after a proven payment history or following receipt of a deposit.

### 3.1.2 Retail Charging

- 16 Section 6.1.2, paragraphs 168 and 169 describe how the application of retail charges by the retail operator influences the NRA's decision to intervene. The measures described here may incentivise an operator to pass on the retail charges to the customer even in cases where previously the operator has decided not to do so. If the operator does this, the NRA may then judge the incident worthy of acting on and require the operator to withhold interconnect payment (removing the financial exposure of the operator to the fraud), whereas if the operator waives payment by the customer the NRA may take no action exposing the operator to having to pay the interconnect charges.
- 17 Even if the operator has charged its customer (which may be a retail customer, but may also be another operator earlier in the traffic chain from which it has received calls for transit/termination) there may be times when an operator and/or NRA would consider it appropriate to invoke the payment withholding process in order to disrupt the fraudsters, and then to refund the operator's customer.
- 18 Paragraph 169 focusses exclusively on a legitimate end user, and needs to be developed to consider a fraudulent end user. The paragraph states *"If the retail operator intends to charge, or has already charged, the full retail price associated with the fraudulent traffic to the end user, the requesting NRA may consider it inappropriate to impose the full rigour of this process..."* If the end user is fraudulent, and has no intention to pay the charges, then the concept of genuine end user harm does not apply, and the full rigour of the process should be imposed to prevent the fraudster from receiving revenue at the other end of the traffic chain.

### 3.1.3 Varying Incentives depending on Operator role

- 19 The operator in the traffic chain with the retail end user as its customer has the greatest incentive, relative to other parties in the traffic chain, to support the proposed process, as it currently suffers the full loss if the end user is fraudulent, and it usually suffers part of the loss even where legitimate end users have been defrauded (e.g. through Wangiri calls or via PBX hacking). There are incidents in which a transit operator may also suffer a loss (e.g. in the case of a dispute with retail operator). The terminating operator in the traffic chain usually currently get paid by the previous party in the chain regardless of whether the traffic was fraudulently generated or not, due to the absence of payment withholding clauses in their bilateral contracts.

### 3.2 ***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.***

- 20 No GSMA response in this section.

**3.3 *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?***

- 21 The consultation paper focusses heavily on legitimate consumers of communications services rather than the perpetrators of fraud, who dishonestly acquire services in order to generate revenue, resulting in losses for operators. Even when legitimate customers are affected by fraudulent schemes (e.g. Wangiri calls, PBX hacking), operators usually also suffer a financial loss, often accompanied by loss of customer goodwill and reputational damage.
- 22 The retail communications industry is also moving progressively towards flat-rate tariffs for international call services, commonly allowing customers to make unlimited calls to various international destinations for a single monthly price. In contrast, international wholesale interconnect voice traffic is metered on a per-minute basis. In this environment, the risk to consumers for international fraudulent calls is reduced, but the risk to operators from fraudulent abuse of such packages is increased. Operators may limit their risk exposure by contractually excluding high-risk destinations in their offers.
- 23 The consultation paper does not mention roaming of mobile subscriptions and there is ambiguity about the responsibilities of operators and the definition of fraud origin with regard to roaming SIMs. Roaming needs to be fully considered from the perspectives of incentives, process, and thresholds for intervention.
- 24 Although the risk of fraud and misuse related to premium rate numbers is not insignificant, the problem of short-stopping and hijacking of other allocated or unallocated portions of national numbering plans is more significant, and is a growing problem. Fraudsters are targeting these numbers because of the increased complexity of blocking hijacked ranges and withholding payment in a hijacking or short-stopping fraud case.
- 25 A single fraud incident may involve a series of calls that originate from the same source, but are carried via multiple different routes to the same destination. This multiplies the intervention effort that would be required from the NRA and increases the number of participants that need to participate in an effective process for call routing determination, number range blocking and payment withholding.

**3.4 *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.***

- 26 In the GSMA's view, the proposed process would add a burden and harm the communications industry by disrupting relationships between communications providers and undermining commercial confidence in the interconnect payment chain. The proposed process risks causing this harm and not achieving its objective of disrupting fraud and misuse. The GSMA's concerns in several areas are described below.

### 3.4.1 Timing

- 27 Whilst this is a regulatory driven initiative, most of the work related to identifying transit carriers will be done by operators and preceding carriers in the traffic chain. The primary obstacle to effectiveness of the proposed process is timing. The consultation paper suggests in section 6.1.4, paragraph 182 that in early cases it may not be possible to be *“totally effective in the objective to ensure the effective disruption of revenue to the perpetrators of fraud or misuse.”* The GSMA is concerned by this declaration, and we believe that the timescales of the proposed process need to be designed with due consideration for existing commercial settlement timescales so that the process will provide an effective deterrent to fraud and misuse.
- 28 To evaluate the obligations of each party to act within prompt timescales and contribute to an effective overall process, the GSMA would like to see example service level agreements, including timescales, that would need to exist between
- NRAs and other EU Member State NRAs
  - NRAs and operators, carriers and service providers within their jurisdiction
  - NRAs or operators and police forces (where necessary).
  - NRAs and the BEREC office
- 29 Since organised fraud is most commonly perpetrated outside working hours (evenings and overnight, weekends, holiday periods), the GSMA would like to understand whether NRAs intend to resource the proposed process during such periods. The example service level agreements requested above should specify expected response times to requests made during such periods.
- 30 Timeframes for responses from NRAs outside of the EU should also be estimated in order to judge the likely effectiveness of intervention in cases where part of the transit of a call takes place outside of the EU.
- 31 The GSMA would like to understand the steps that would be taken by a NRA if participants in the process from which it has requested information are not able to comply with the service level agreements..

### 3.4.2 Realistic Example

- 32 The example in section 5.3.1 is useful for illustrating the process, but is simple and not indicative of a real scenario. Additional examples should be developed and described that include:
- At least three carrier businesses in different countries
  - Parties outside of the EU
  - Roaming
  - Short-stopping with the consent of the number range holder, where the dialled number is unrelated to the point of termination.
  - Short-stopping without the consent of the number range holder (hijacking)
  - Calls to unallocated number ranges
- 33 Expected, best case and worst case timelines for information requests and responses between parties should be applied to these examples in order to compare the total



period required to complete the process against normal wholesale and retail settlement timescales.

### **3.4.3 Information Required**

34 Section 6.1 (paragraph) and section 6.1.5.4 (paragraph 203) mention the need for a minimum standard of information to be exchanged between NRAs, highlighting the following data elements:

- Nature of fraud or misuse
- Time and date of incident start time
- Originating number(s)
- Terminating number(s)
- Transit and terminating operators involved in the transmission of the call(s)
- Call detail records (CDRs)
- Supporting information demonstrating basis of initiation of case by originating NRA (e.g. confirmation of police reporting where applicable)

BEREC would need to develop and formally confirm the minimum standard of information to be exchanged and the associated format. A common standard or template would need to be defined, and operators should be consulted as part of this task, since they will be expected to provide most of the information.

### **3.4.4 Roaming**

35 International roaming for mobile telephony customers needs to be incorporated into the proposed process. The GSMA has observed that roaming is often used by fraudsters to try and extend the period within which they can abuse dishonestly acquired services before detection. In recent years, mobile network operators have invested in a rapid inter-operator process for detecting fraud by roaming users to minimise this risk, but fraud perpetrated while a SIM is roaming remains a concern for operators. The proposed BEREC process should therefore fully address roaming, and describe the steps to be followed in the scenarios below:

- A subscription (used legitimately or fraudulently) from a mobile network operator located in one EU Member State suffers or perpetrates fraud or misuse when roaming in another Member State. In this scenario, is the originating country considered to be the country of origination of the SIM card, or the country of origination of the calls? Which NRA and which police force should the fraud incident be reported to?
- A subscription (used legitimately or fraudulently) from a mobile network operator located outside of the EU suffers or perpetrates fraud or misuse when roaming in a Member State.
  - Will the mobile network operator in the country outside of the EU need to directly approach the NRA of the Member State in which the calls were made? Alternatively, will that operator need to request that its EU-based roaming partner, on whose network the calls were made, approach the EU Member State NRA on behalf of the mobile network operator outside of the EU?

- A subscription (used legitimately or fraudulently) from an EU-based mobile network operator suffers or perpetrates fraud or misuse when roaming outside of the EU.
  - How would the NRA of the Member State propose to intervene and request blocking or payment withholding if the fraud or misuse was not perpetrated within its jurisdiction?

Will the NRA intervene in such cases? If such scenarios are not addressed, fraud will adapt to exploit this process weakness, through utilisation of networks in countries bordering EU Member States or beyond.

### 3.4.5 Police Reporting

- 36 Mobile network operators have expended considerable time and effort in the past trying to report telecoms fraud to the police. If police reporting is a prerequisite for NRA intervention, then police reporting processes should be streamlined in order to support the efficiency of the wider BEREC co-operation process. It would be helpful if NRAs could nominate a single police point of contact in their jurisdiction and ensure that the point of contact is familiar with its role in the BEREC co-operation process.
- 37 The GSMA encourages BEREC to request greater police co-operation amongst Member States to tackle the organised criminals who illegally perpetrate fraud across multiple jurisdictions.

### 3.4.6 Control over Blocking of Number Ranges

- 38 With reference to section 2.3.1, paragraph 24, and recital 46 of Directive 2009/136/EC, *"a single market implies that end-users are able to access all numbers included in the national numbering plans of other Member States and to access services using non-geographic numbers within the Community, including, among others, freephone and premium rate numbers"*. The paragraph also states *"Cross-border access to numbering resources and associated services should not be prevented, except in objectively justified cases, for example to combat fraud or abuse (e.g. in connection with certain premium-rate services)..."* It is not clear from the proposal whether operators are permitted to block number ranges that are identified as fraudulent, and clarification from BEREC on this point is requested.
- 39 The proposal appears to suggest that the NRA in the terminating country will request blocking of numbers on a case by case basis. This will have no impact on hijacking / short stopping as the call would not reach the destination the number range was intended for. Where a mobile operator has evidence that a number range is a target to fraudsters then it will want to be able to block number ranges. Failure to do this will increase the overall fraud cost to operators.
- 40 Mobile network operators consider it essential that they retain the ability to choose whether or not to block (at least temporarily) or unblock access to number ranges or services, depending on their independent commercial assessments of the associated fraud risk. Operators already assess the risk of fraud and misuse and block access to ranges and services (where feasible) to protect their customers and their business if they consider the risk of fraud or misuse to be significant. Operators support swift

intervention in cases of fraud to ensure the protection of their customers, as opposed to unnecessary delaying in order for an NRA or other body to build evidence for a case.

- 41 Blocking access can only be done where it is technically feasible to do so. In some cases, blocking may only be able to be applied to broad ranges of numbers, even though such blocking could have unintended detrimental consequences by affecting innocent parties. Within mobile networks, blocking access to selected numbers or ranges for roaming end users is more difficult than doing so for end users located within their home network.

#### **3.4.7 Wangiri Fraud Type**

- 42 The GSMA believes that the process will be ineffective at mitigating Wangiri fraud based on the current fraud detection configurations used by mobile network operators, for the following reasons:
- Most fraud management systems deployed by operators are designed to detect anomalous usage at calling number (A-number) level not called number (B-number) so operators would need to make a significant change to proactively detect Wangiri fraud.
  - It is more realistic that the detection is driven by a customer complaint after the customer receives an invoice.
  - As detection is driven by customer invoicing, at this point the interconnect invoices and consequently the fraudster will most likely have been paid.

#### **3.4.8 Need for Consistency**

- 43 The GSMA believes that this process cannot be effective unless all NRAs follow the same rules. In a typical cross border case of suspicious or unusual traffic, the NRA with jurisdiction over the originating operator may decide to intervene under the terms of the proposed process, whereas the NRA regulating the terminating operator may decide not to intervene. Thus, the originating operator may withhold revenue from the terminating operator, who in turn is unable to withhold payment to a service provider and will therefore suffer a financial loss. This may be made even worse if transit providers are also involved, as those organization may have nothing to do with the jurisdiction where the alleged fraud or misuse originated or terminated. Thus without a consistent process, operators and transit carriers that happen to carry certain traffic may stand to lose all of the associated revenue, with no means to predict or control this risk exposure. This is an unacceptable scenario, which risks strongly damaging commercial relations between communications providers.

#### **3.5 *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.***

- 44 There is no single view amongst mobile operators within the GSMA regarding the proposed threshold level.

- 45 One view is that the proposed thresholds are too low to be practical, as they will generate an excessively large volume of cases to be handled, placing a significant burden on NRAs, the BEREC office, and operators.
- 46 Another view is that the thresholds are reasonable, since to make them higher would increase the loss to legitimate end users. Higher thresholds would give fraudsters a profitable window within which to operate without fear of intervention. However, it could be argued that fraudsters will adapt to operate beneath any practical threshold that is set for intervention by perpetrating an increased number of fraud incidents with a lower associated value per incident. One option would be to set the thresholds higher than proposed by BEREC when the process is first introduced, to avoid process participants having to deal with an excessive number of cases while the process is new. When the process has been in place for a certain period, and is working efficiently and effectively, then it may be appropriate to lower the threshold and intervene in more incidents.
- 47 Through the use of fraud management systems and close monitoring, mobile operators are often able to detect fraudulent traffic on their networks as soon as it begins to occur. In such cases, they will intervene to prevent further calls and associated loss, and to block the associated subscriptions. They may also monitor or block further calls to the terminating numbers from their network, if deemed to be at high-risk of repeated fraud. Where this type of fraud management is done efficiently, it is likely that the retail charges that the operator would have applied will be small and will not exceed the threshold for NRA intervention. Conversely, operators that are less effective at detecting fraud will host greater quantities of fraudulent traffic that will exceed a specific threshold more frequently. If NRA intervention allows these less efficient operators to withhold payment and avoid a loss in such cases, they have little incentive to invest in more effective fraud detection.
- 48 The GSMA believes that a threshold based on the charges that the retail operator intends to apply to the retail end user for fraudulent traffic is unsuitable by itself, and that the NRA decision to intervene should be based on an augmented combination of information, both quantitative and qualitative, that indicates a fraudulent pattern of activity. For example, factors such as unusually high traffic volumes (minutes of usages or number of calls), calls to destinations that have experienced fraud in the past, or the absence of meaningful matter conveyed on the calls (information, music or sound signals which have a purpose beyond simply keeping the connection open for revenue earning reasons) should be taken into consideration by an NRA considering intervention.

**3.6 *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.***

- 49 Typical commercial interconnection agreements contain clauses defining deadlines for payments and processes and timescales for the settlement of disputes. These clauses will influence the ability of operators to withhold interconnection revenues. Application of the proposed BEREC process for payment withholding causing a breach of these

clauses is likely to trigger commercial disputes between interconnected partners. This is especially likely if those parties are in different countries within or outside the EU where the NRAs have different approaches to intervention.

**3.7 Are there other circumstances at which NRAs should consider intervention under Article 28(2)? Please give reasons for your response.**

- 50 Member State NRAs should look at the retail businesses and service providers linked to recurring fraud events in their countries and work with them to determine the cause of recurring frauds. The process proposed by BEREC could be selectively applied in such scenarios, in combination with other investigative support.

## **4 Additional Comments**

### **4.1 General Comments**

- 51 Section 6.1.4, paragraph 182 finishes, *“An inability to disrupt the overall flow of money would not be considered as precluding the use of this process to the extent possible.”* Further clarification of the meaning of this statement is requested with reference to the objectives outlined in section 2.1 of the consultation paper. The key measurement of success for this process will be whether it has prevented the fraudster from receiving revenue. If that is not achieved, then the cost and effort to follow the proposed process amongst NRAs and operators in the traffic chain is not justified. The GSMA believes that if the process is unable to disrupt the money flow to the perpetrators of fraud and misuse, it should not be implemented.
- 52 In section 5.3, paragraph 126, BEREC proposes a confidential reference database of cases of fraud or misuse reported under the process managed by NRAs in each country. Whilst this may be appropriate for consumer reports, the GSMA would oppose applying confidentiality to reports from operators if this means there is no visibility or transparency and relies upon NRAs to assess the effectiveness of the process.
- 53 Member States should be entitled to evaluate whether the provision of accessibility to certain numbers in other Member States is correctly in balance with the associated risk of fraud and the real demand from the end users to access those numbers.

### **4.2 Suggestions to Improve Proposed Process**

#### **4.2.1 Centralised Reporting and Broadcast Notification**

- 54 BEREC recognises that the best results are achieved if the flow of money is disrupted as early as possible but the GSMA believes that the best way to disrupt the money flow and protect the interests of consumers is to prevent the loss occurring. If there was a common, central reporting process it would be possible to report fraud/misuse and simultaneously alert both NRAs and operators to current activity via a broadcast model, subject to data protection legislation. Operators may then be in a position to better protect consumers by restricting or denying access to exploited services or numbers and NRAs would receive much faster notice of apparent abuse within their jurisdiction.

- 55 If operator reports were made in a common agreed format and reported simultaneously to originating and terminating NRAs, the terminating NRA could, in the interests of speed and in cases where short-stopping or hijacking have not occurred, issue an interim freezing notice whilst the facts are confirmed and reviewed and a decision is made.

### **4.3 Other Suggestions**

- 56 BEREC is proposing a complex and high-effort process to address the problem of fraud and misuse. It should also consider the following suggestions that may help to address the problem with less effort.

#### **4.3.1 Stricter National Number Range Management**

- 57 Operators and transit carriers carry calls in good faith, unaware that they may sometimes be fraudulent or that the calls will be mis-routed further on in the traffic chain and terminate in a country other than the country from whose numbering plan the called numbers are taken (short-stopping). The GSMA believes that numbering resource misuse is an enabler for fraud, making fraud easier to conduct, more profitable and less subject to prosecution. NRAs can help communications providers to reduce the risk of number resource misuse such as short-stopping, hijacking and abuse of unallocated number ranges by enforcing stricter management of national numbering resources, as outlined below:
- Member State NRAs should closely manage number range allocations within their own countries and ensure that their national numbering plans are complete, detailed, up to date, publicly available via their websites and maintained. Comprehensive and correct data is especially valuable in relation to number ranges assigned to special services. This data will allow operators and carriers to identify and investigate potentially fraudulent traffic, especially where short-stopping or hijacking of unallocated number ranges is occurring.
  - Member State NRAs could implement stricter controls over the assignment of number ranges to applicants in their own countries and ensure that the ranges are used for the purpose for which they have been assigned.
  - Member State NRAs could implement stricter controls over leasing of number ranges by number range assignees to third parties, often for use in providing premium or other special services. Where such leasing is permitted by the NRA, the original number range assignee should be required to notify the NRA of this, so that details of the affected number ranges and of the services available via those ranges can be added to the national numbering plan or made publicly available through some other means.