

# Operator Information Notice



An Coimisiún um  
**Rialáil Cumarsáide**  
Commission for  
**Communications Regulation**

## Regulation 23(2) Process An Operator's Information Note

<b>Reference</b>	ComReg 18/119
<b>Version</b>	FINAL
<b>Date</b>	20 December 2018

## Contents

1	Introduction.....	3
2	Background .....	4
3	Objective of the Regulation 23(2) Process.....	5
4	Considerations for intervention in misuse cases.....	6
5	Recommendations for Operators .....	8
6	Process for investigating misuse cases .....	9
Appendix: 1	Relevant Information.....	11
Appendix: 2	Operator misuse form .....	12

# 1 Introduction

1. In 2011, an amended version of Article 28(2) of the Universal Service Directive came into force, the revised provision of which related to end-user protection in the case of fraud or misuse.
2. Article 28(2) of Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (the “Universal Service Directive”) establishes a requirement for Member States to *“ensure that the relevant national 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”*.
3. Article 28(2) was transposed into Irish law by Regulation 23(2) of the European Communities (Electronic Communications Networks and Services) (Universal Service and User’s Rights) Regulations 2011 (the “Universal Service Regulations”) (“Regulation 23(2)”). Regulation 23(2) states that:

*“The Regulator may require undertakings providing public communications networks or publicly available electronic communications services to block, on a case by case basis, access to numbers or services where this is justified by reason of fraud or misuse and to require undertakings to withhold relevant interconnection or other service revenues.”*
4. The “Regulator” for these purposes is the Commission for Communications Regulation (“ComReg”).
5. This Information Note describes ComReg’s policy and the process for managing cases of fraud or misuse. ComReg will normally adhere to this process but alternative approaches may be used depending on the circumstances of the case.
6. Incidents which require the use of Regulation 23(2) are often cross border in nature and include operators in other Member States and in countries outside the EU. Accordingly, the Body of European Regulators for Electronic Communications (“BEREC”) produced a guidance paper in 2013: *Article 28(2) Universal Service Directive: a harmonised BEREC cooperation process - BEREC Guidance* (the “BEREC Guidance Paper”)<sup>1</sup>.
7. The BEREC Guidance Paper outlines the BEREC process for cross border regulatory cooperation in cases of fraud or misuse which informs this document.

---

<sup>1</sup> Document number: BoR (13) 37 Document date: 07.03.2013  
[http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/regulatory\\_best\\_practices/guidelines/1187-draft-berec-guidance-paper-article-282-universal-service-directive-a-harmonised-berec-cooperation-process](http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/1187-draft-berec-guidance-paper-article-282-universal-service-directive-a-harmonised-berec-cooperation-process)

## 2 Background

8. ComReg, by intervening in cases of misuse, aim to protect end-users, and in some circumstances Operators, from exposure to the financial liability that occurs as a result of the alleged fraud or misuse.
9. In deciding whether an incident constitutes a fraud or misuse within the meaning of Regulation 23(2), ComReg is guided by the BEREC Guidance Paper. As noted in the BEREC Guidance Paper, *“neither of the terms “fraud” nor “misuse” were specifically defined within the Universal Service Directive”*. The BEREC Guidance Paper goes on to state that *“for this purpose, and for the purposes of providing guidance in the context of Article 28(2) USD and without prejudice to new forms of fraud or misuse that could appear in the future, a non-exhaustive list of situations dealt with by operators and authorities that could qualify as fraud or misuse can be illustrated by the following examples...”*.
10. The following examples are provided in the BEREC guidance paper:
  - a. Use of numbering intended for an end-user for the provision of services not included in the national numbering plan (e.g. auto-dialling);
  - b. The use of an unallocated number by a party without the consent of the allocating entity (e.g. short-stopping in the same country, in another EU country or beyond EU borders);
  - c. The use of a number by a third party to whom the number was not allocated, without the consent of the party to whom it was allocated (e.g. phone hijacking, or PBX hacking);
  - d. The generation of a call with a Calling Line Identifier (A-number) which is also used for premium rate services and when subsequently used by the called party it results in an inappropriate cost to the original called party (Wangiri fraud);
  - e. The use of an allocated number without obeying transparency obligation (e.g. omit or include an inadequate warning of the tariff, price announcement);
  - f. Artificial inflation of traffic (“AIT”) or causing AIT.
11. The majority of incidents that are brought to ComReg’s attention relate to PBX hacking. This type of incident typically involves a third party hacking into a business telephone system (PBX) and causing high volumes of outgoing calls to be made to international destinations with high termination rates. The third party will usually receive a payment for the calls being terminated on these numbers.

## 3 Objective of the Regulation 23(2) Process

12. ComReg will primarily use its Regulation 23(2) powers for the purpose of protecting end-users. ComReg aims to protect end-users from the financial losses associated with misuse incidents. In addition it is hoped that ComReg's actions, with the assistance of industry using a coordinated approach, will reduce the number and impact of incidents in the future.
13. There can be difficulties in operators seeking to recover the costs of calls associated with fraud or misuse cases where payments have already been made, due to contractual issues. ComReg recommends that operators review their interconnection agreements with their interconnect operators such that the charges can be stopped and/or reimbursed. Such changes may negate the requirement for regulatory intervention in the future and could assist with disrupting the flow of money to the perpetrator(s) of fraud and/or misuse.
14. It would not be practical or proportionate for ComReg to intervene in all incidents, and in accordance with the BEREC Guidance Paper, consideration will be given to a number of factors, including the financial impact of the incident, when considering whether to intervene. Therefore ComReg will consider, on a case by case basis, whether the use of Regulation 23(2) is practical and proportionate.
15. ComReg wishes to raise awareness of misuse and fraud incidents among end-users and operators with a view to enhancing security measures on end-users equipment and enhancing monitoring systems by operators.<sup>2</sup>

---

<sup>2</sup> See in this regard paragraph 22 and paragraphs 214-219 of the BEREC guidance paper.

## 4 Considerations for intervention in misuse cases

16. In making a decision to use its Regulation 23(2) powers, ComReg will consider among other things, the following:

- a. Economic Thresholds
- b. Timeliness of reporting
- c. Whether the end-user has made a complaint to An Garda Síochána
- d. End-user protection

These are described in the following sections.

### 4.1 Economic thresholds

17. In line with the BEREC guidance paper, it may not be proportionate for ComReg to intervene in cases where the total wholesale costs for the incident, payable by the retail service provider, are less than €5,000. Where the total wholesale costs are below this level, ComReg may consider intervention where the total wholesale costs exceed a factor of [3] times the relevant end-user's normal bill but not if the costs are below €1,500. Below €1,500 ComReg may decide that it is not appropriate to intervene under Regulation 23(2).

18. Additionally, in line with BEREC guidance, it is also proposed that when determining whether to intervene for an individual transit operator in certain circumstances<sup>3</sup>, ComReg may consider the amount to be withheld by an individual operator relative to any evidence provided by an operator regarding the administrative cost of withholding. This will be dealt with on a case-by-case basis. This consideration will have due regard to the overall objectives of end-user protection and blocking of revenues to the hacker. If ComReg does not intervene in relation to one or more transit operators, the wholesale costs of those operators will still be considered when determining whether the overall wholesale costs for the incident exceeds the €5,000 threshold.

### 4.2 Timeliness of reporting

19. All misuse incidents should be reported by the retail operator to ComReg using [misuse@comreg.ie](mailto:misuse@comreg.ie), without undue delay, but no later than 15 days following detection of the incident.

---

<sup>3</sup> In some incidents ComReg has observed multiple separate wholesale traffic routes and payment paths over multiple operators. In these circumstances, one or two operators will carry the bulk of the calls with a very small number of calls being carried by other operators. In such circumstances, individual operators with very low call volumes will have very low wholesale costs as a result.

20. The effectiveness of any intervention by ComReg may be negatively impacted by delays in reporting the incident or providing the relevant information.
21. The inability to stop all payments within the interconnect payment chain may not be a proportionate reason to prevent ComReg intervening in a case of misuse. However any preventable delays in providing information to ComReg will be considered when deciding whether or not to intervene. ComReg will consider each case on its individual merits.

### **4.3 Whether the end-user has made a complaint to An Garda Síochána**

22. The end-user should be advised to contact An Garda Síochána to report the incident without undue delay. The end-user will be provided with a Gardaí PULSE number which should be submitted by the Operator when reporting an incident to ComReg, or as soon as possible thereafter. Failure to report a matter to the Gardaí will prevent ComReg investigating a case under Regulation 23(2).

### **4.4 Whether the end-user has experienced previous incidents of misuse**

23. ComReg may not intervene in cases where the end-user was aware of risks and/or inadequacies in their security systems but failed to remediate them so as to prevent or mitigate against any further incidents of fraud or misuse.
24. In particular, ComReg will normally not investigate a case where the end-user experienced previous incidents but subsequently failed to take appropriate steps and/or remedial action to ensure adequate security measures are present on their telecommunication systems.<sup>4</sup>

### **4.5 End-user protection**

25. The primary focus of this process is to protect end-users from the consequences of fraud and misuse. This protection is provided directly by intervention with the retail operator. This can result in ComReg requiring interconnection or other service revenues to be withheld.
26. When forming a view whether to intervene in a case, ComReg will consider what charges, if any i.e. wholesale costs, retail costs, the retail operator intends to charge the end-user for the calls.

---

<sup>4</sup> See in this regard paragraph 217-218 of the BEREC Guidance Paper.

## 5 Recommendations for Operators

27. At all times appropriate measures should be taken by the end-user, the PBX owner and maintainer and the retail and wholesale operators, to prevent incidents occurring and to limit the severity and impact of any incidents.
28. Operators should implement reliable fraud monitoring systems and procedures, on a 24 hour basis, to detect unusual activity such as:
- a. calls to unusual destinations,
  - b. high volumes of calls in a short period of time; or
  - c. high volumes of calls outside of normal working hours.
29. Measures should be taken to detect and stop an incident at the earliest possible opportunity, especially those incidents occurring outside of normal working hours.
30. Where an operator identifies unusual activity, the incident should be stopped and the end-user advised as soon as possible. The end-user should also be advised to report the incident to An Garda Síochána.
31. ComReg should be notified of the incident without undue delay. ComReg should be provided with a list of the Call Detail Records (“CDRs”) for the incident, to include:
- a. The originating number(s) (A Number);
  - b. The terminating number(s) (B Numbers);
  - c. Call dates and times,
  - d. Call destinations,
  - e. Wholesale and retail costs,
  - f. Call durations; and
  - g. Interconnect operators in the chain.
32. Retail operators should regularly provide briefing material to their business customers outlining the potential risks and suggesting preventative measures that can be undertaken by the end-user to mitigate these risks.<sup>5</sup>
33. ComReg would encourage retail operators to ensure that their customers are aware that ComReg may not intervene in all cases and that it is important that appropriate security measures are implemented on their equipment.

**NOTE** Operators may be left liable for all or a portion of the costs if ComReg decides it is not proportionate to intervene in the case.

---

<sup>5</sup> See paragraph 219 of the BEREC Guidance Paper.



# 6 Process for investigating misuse cases

## 6.1 Case initiation

34. The retail operator should notify ComReg of incidents of alleged fraud or misuse (PBX Hacking, Wangiri fraud, Roaming, Artificial Inflation of Traffic (“AIT”)) by emailing [misuse@comreg.ie](mailto:misuse@comreg.ie) using the Operator Misuse Form<sup>6</sup>.

**NOTE 1 ComReg should be notified of a potential incident of misuse and provided with the relevant information without undue delay.**

35. Any outstanding information will be requested from the retail operator or subsequent operators in the chain who have been identified as providing interconnection services relating to the incident.

36. All relevant information<sup>7</sup> should be submitted to ComReg as soon as possible after the incident is detected, but no later than 15 calendar days after the incident is detected.

37. ComReg will review the case information and make a decision to:

- a. Not intervene and close the case; or
- b. Intervene in the case subject to the following decisions:
  - i. that there has been misuse of an Irish number within the meaning of Regulation 23(2) of the Universal Service Regulations; and
  - ii. to require the retail operator, and any interconnect operators within the jurisdiction, to withhold interconnection payments and other service revenues for the relevant calls to its interconnect operator(s) pursuant to Regulation 23(2) of the Universal Service Regulations.

**NOTE It may not be proportionate for ComReg to use their Regulation 23(2) powers in every instance and ComReg will make a decision on a case by case basis.**

## 6.2 Notification of initial decision

38. In the event that ComReg decides not to use their Regulation 23(2) powers, ComReg will notify the retail operator(s) in writing (by email), of the decision not to intervene.

39. In the event that ComReg decides to utilise their Regulation 23(2) powers, ComReg will notify the relevant operator(s), by way of email and registered letter, of the decision to utilise Regulation 23(2) (the “Interim Requirement”).

---

<sup>6</sup> See Appendix: 2

<sup>7</sup> See Appendix: 1

40. The Interim Requirement will remain valid for four months from the date the letter is issued.
41. Where appropriate ComReg may notify the National Regulatory Authority (“NRA”) of the relevant EU interconnect operators of its decision to use its Regulation 23(2) powers. This will enable NRAs in interconnect countries to decide on the appropriate action in their country of jurisdiction.

### **6.3 Continuing investigation during the interim period**

42. Operators and NRA’s have two months from the date the Interim Requirement is issued to make representations to ComReg.

### **6.4 Decision on whether to make permanent the Interim Requirement**

43. ComReg will consider any representations made by operator/s and NRAs when making a decision to confirm the provisional finding of misuse and make the Interim Requirement permanent, or to allow it to expire.

### **6.5 Notification of final decision**

44. ComReg will formally notify the retail operator and relevant interconnect operators of the decision to amend or make permanent the Interim Requirement, or of the decision to allow the Interim Requirement to expire.

### **6.6 Change to the process**

45. The process set out above is subject to change depending on the circumstances of each individual case. The process will be reviewed and may be updated from time to time, as appropriate.

## Appendix: 1 Relevant Information

A 1.1 The following information is mandatory in order for ComReg to carry out an investigation into a case of alleged fraud and/or misuse:

- Call Detail Records (CDR's) for the incident in an Excel file;
- Wholesale costs for the relevant calls, excluding VAT;
- Retail costs for the relevant calls, excluding VAT;
- Average monthly retail bill (€) (ex VAT) - Required if wholesale costs for relevant calls < €5,000)
- Interconnect operators – who are the interconnect operators<sup>8</sup> and what portion of the calls are associated with each operator;
- Garda PULSE Number;
- Date/s that payment for the relevant calls is due to interconnect operators;
- Confirmation from the retail operator that they are not responsible for the maintenance of the security of the end-users PBX system;
- What costs, if any, will the retail operator charge if ComReg does not agree to intervene and what costs, if any, will they charge if ComReg does agree to intervene?

---

<sup>8</sup> When an onward operator has operations within Ireland, and outside of the state, the jurisdiction within which the interconnect operator is operating should also be noted.

## Appendix: 2 Operator Misuse Form

### Primary Operator Misuse Notification Form

Please complete the form and return to ComReg no later than 15 calendar days after incident is detected and stopped.

Failure to provide the relevant information in a timely manner may result in ComReg being unable to take action in relation to the case.

<b>Operator contact details (name and address)</b>	
<b>Retail operator (if different from above)</b>	
<b>End-user business name</b>	
<b>Garda Reference Number</b>	
<b>Call Details</b>	<i>To be sent electronically on excel spread sheet</i>
<b>Wholesale costs for Relevant Calls (€) (ex VAT)</b>	
<b>Retail costs for Relevant Calls (€) (ex VAT)</b>	
<b>Average Monthly Retail Bill (€) (ex VAT)</b>	<i>(Required if Wholesale costs for Relevant Calls &lt; €5,000)</i>
<b>Interconnection Operators - Ireland</b>	
<b>Interconnection Operators – Outside Ireland</b>	
<b>Portion of costs assigned to each interconnect operator</b>	
<b>Date/s that payment is due on the relevant calls to Interconnect Operators</b>	
<b>Do you maintain the security of the end-users PBX?</b>	
<b>What costs will you charge the end-user if ComReg intervenes?</b>	
<b>What costs will you charge the end-user if ComReg does not intervene?</b>	