

Operator Information Notice



An Coimisiún um
Rialáil Cumarsáide
Commission for
Communications Regulation

Fraudulent and/or Misuse of Numbering Resources - Regulation 83(2) Process

An Operator's Information Note

Reference	ComReg 18/119R
Version	Final
Date	25 October 2023

Contents

1 Introduction	3
2 Background	4
3 Objective of the Regulation 83(2) Process	5
4 Considerations for intervention in misuse cases.....	6
5 Requirements for Operators.....	8
6 Process for investigating misuse cases	9
Appendix: 1 Relevant Information.....	11
Appendix: 2 Operator Misuse Form	12
Appendix 3 Advice to End Users.....	13

1 Introduction

1. The communications regulatory framework, established by the European Electronic Communications Code ('**EECC**')¹, was transposed, in part, into Irish law by the European Union (Electronic Communications Code) Regulations 2022, S.I. No., 444 of 2022 (the '**ECC Regulations**').
2. Regulation 83(2) of the ECC Regulations replaces Regulation 23(2) of the European Communities (Electronic Communications Networks and Services) (Universal Service and User's Rights) Regulations 2011 (the "Universal Service Regulations"). Article 83(2) of the EECC Regulations states:

83(2) The Regulator may require providers of public electronic 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 that in such cases those providers withhold relevant interconnection or other service revenues."
3. The "Regulator" for these purposes is the Commission for Communications Regulation ("ComReg").
4. This Information Note describes ComReg's policy and the process it follows 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.
5. Incidents which require the use of Regulation 83(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")².
6. The BEREC Guidance Paper outlines the BEREC process for cross border regulatory cooperation in cases of fraud or misuse which informs this document. While the BEREC guidance paper relates to Article 28(2) of Universal Service Directive, ComReg believes the theme of this guidance in principle remains relevant.
7. The link below can be used to access the "Misuse" section of ComReg's website:
<https://www.comreg.ie/industry/electronic-communications/compliance-enforcement/misuse/>

¹ Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code.

² 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-draftberec-guidance-paper-article-282-universal-service-directive-a-harmonised-berec-cooperation-process

This section of the website contains :

- a The full Regulation 83(2) Operators Information Note
- b A summary of ComReg's powers relating to the Misuse process
- c Advice to PBX owners
- d The Operator Misuse Notification Form

2 Background

8. ComReg, by intervening in cases of misuse, aims 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 83(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) USD³ 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.

³ Universal Service Directive

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 83(2) Process

12. ComReg will primarily use its Regulation 83(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 83(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.⁴

⁴ 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 83(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 will consider the circumstances of the incident and may decide that it is not appropriate to intervene under Regulation 83(2).

18. Additionally, in line with BEREC guidance, when determining whether to intervene for an individual transit operator⁵, 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, without undue delay, but no later than 15 days following detection of the incident.

20. The effectiveness of any intervention by ComReg may be negatively impacted by delays in reporting the incident or providing the relevant information. The frequency of

⁵ 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.

paying revenues to onward operators will obviously impact on the ability to withhold revenues.

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 Service Provider should advise the end-user 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 83(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.⁶

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.

⁶ See in this regard paragraph 217-218 of the BEREC Guidance Paper.

5 Requirements 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 flag a range of unusual calling patterns, marked by a high frequency of:
 - a. Calls to international destinations commonly associated with fraudulent activities, particularly if these destinations are not usually contacted by the end-user.
 - b. Calls made during hours when the end-user's business is generally closed.
 - c. Calls to premium or high-cost numbers that fall outside the end-user's usual call patterns.
 - d. Calls of short duration, in quick succession and within a short timeframe.
29. Measures should be taken to detect and stop an incident at the earliest possible opportunity, especially those incidents occurring outside of the normal working hours of the end-user concerned.
30. Where an operator identifies unusual activity, immediate steps should be taken to prevent further activity and the end-user advised as soon as possible, including reporting the incident to An Garda Síochána and obtaining a Pulse Number.
31. ComReg should be notified of the incident without undue delay. ComReg should be provided with a list of the relevant individual Call Detail Records (“CDRs”) in an Excel file in the following format:
 - 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 risks⁷. Appendix 3 of this document includes advice to end-users to help them mitigate risks relating to potential Misuse of PBX's, as well as advice on responding to an incident.

⁷ See paragraph 219 of the BEREC Guidance Paper.

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

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 and attaching the Operator Misuse Form⁸. Where the submitted Operator Misuse Form is incomplete due to, for example, unavailable information at the time of submission such as details of PBX installation or Garda Pulse Number, a fully completed form should follow as soon as possible.
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 information⁹ 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 decide to:
 - a. Not intervene and close the case; or
 - b. Intervene in the case subject to the following decisions:
 - i. that there has been a misuse of an Irish number within the meaning of Regulation 83(2) of the ECC 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 83(2) of the ECC Regulations.

NOTE It may not be proportionate for ComReg to use their Regulation 83(2) powers in every instance and ComReg will make a decision on a case by case basis.

⁸ See Appendix: 2

⁹ See Appendix: 1

6.2 Notification of initial decision

38. In the event that ComReg decides not to use its Regulation 83(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 its Regulation 83(2) powers, ComReg will notify the relevant operator(s), by way of email, of the decision to utilise Regulation 83(2) (the “Interim Requirement”). The Interim Requirement will remain valid for four months from the date the letter is issued.
40. Where appropriate ComReg may notify the National Regulatory Authority (“NRA”) of the relevant EU interconnect operators of its decision to use its Regulation 83(2) powers. This will enable NRAs in the 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 deciding whether 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 ComReg requires responses to all sections of the Operator Misuse Form in order to carry out an investigation into a case of alleged fraud and/or misuse. This includes the following information:

- Call Detail Records (CDR's) for the incident in an Excel file. The fields required are described in Section 5 of this document;
- Wholesale cost for each relevant call, excluding VAT;
- Retail cost for each relevant call, excluding VAT;
- Where the total wholesale value of the relevant calls is <€5,000, the estimated average monthly retail bill (€) (ex VAT) should be provided;
- Interconnect operators – provide details of the interconnect operators¹⁰ 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. ComReg cannot issue a withhold notice once payment is made to an ongoing operator;
- Confirmation from the retail operator that they are not responsible for the maintenance of the security of the end-users PBX system;
- The costs, if any, the retail operator will charge if ComReg does not agree to intervene, and the costs, if any, that will be charged if ComReg does agree to intervene.

¹⁰ 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 *as per guidance in ComReg 18/119R (An Operator's Note)* and return to ComReg no later than 15 calendar days after incident is detected and stopped.

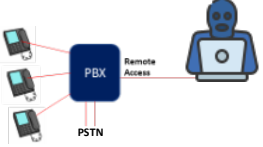
Failure to provide the relevant information in a timely manner may result in ComReg being unable to take action in relation to the case.

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

Appendix 3 Advice to End Users

PBX Hacking – ComReg advice to PBX Owners





What is a PBX?

A PBX (private branch exchange) is a telephone system to manage an organisation's phone calls. PBX owners include businesses, offices and schools. A PBX is made up of hardware and software that connects to communication devices such as telephones, hubs, switches, routers, etc. The PBX may be in the organisation's premises, or it may be a virtual PBX hosted by a communications company. The PBX owner is responsible for the security of PBX's on premises.

What is a PBX Hacking?

Hackers, located anywhere in the world, access a PBX usually through an unprotected remote access such as:

1. a number on the PBX which is intended for use by the PBX maintainer or administrator,
2. services provided by the PBX, for example voicemail.

The Hacker forces the PBX to make international calls, the PBX owner will be billed for these calls.

How can PBX Hacking generate profits?

A hacker takes advantage of telephone calls transiting through a chain of several International Networks. Each transit carries a handling charge which is paid by the network handing over the call to the next network in the chain. Hackers normally dial countries that are the most expensive but seldom called destinations, because the margins are higher than frequently called destinations. The capability to detect and regulate fraudulent calls varies across countries. This may influence a hackers call destination. The revenues will be paid between the international networks but ultimately it is the caller who bears the cost. Hackers can use call generating and call answering equipment to make multiple short duration calls to escape detection and maximise revenue.


How will you know if your PBX has been hacked?

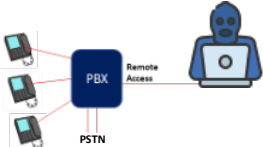
Telecommunications providers are aware of the problem and have implemented procedures to identify suspect international call patterns. These patterns are normally identifiable as repeated short duration calls to international destinations seldom called from Ireland. When telecommunications providers identify suspect call patterns, they normally block international calls from that PBX immediately and notify the PBX owner as soon as possible.

How can a PBX owner minimise the risk of a Hacking Incident?

1. Ensure all remote access circuits have strong password protection, including voicemail access. Be sure to change passwords regularly.
2. Use an approved PBX provider / maintainer. Confirm that they have implemented adequate password protection on their remote access to the PBX.
3. Disable or restrict access to countries that staff don't need to contact. The vast majority of hacked calls are made to destinations that are seldom called from Ireland.
4. Ensure that all security recommendations from your PBX supplier are followed.

PBX Hacking – ComReg advice to PBX Owners





What should a PBX Owner do when notified of a Hacking Incident?

1. When notified by your telecommunications provider of a hacking incident it is advisable to follow their directions and help them to limit the impact of the incident.
2. Hacking is a criminal offence so report the incident immediately to the Gardai and obtain a Garda Pulse Number (a number allocated to the reporting of the incident).
3. Provide the information below to your telecommunications provider as soon as possible. Delays can prevent ComReg intervention
 - End User Details
 - PBX details
 - Garda Pulse Number
4. Contact your PBX maintainer for a security review.

What can ComReg do?

When requested by a telecommunications provider, ComReg can review a hacking incident with the objective of protecting end users where appropriate and proportionate. ComReg can, under Regulation 83(2) of the European Union Electronic Regulations Code Regulations 2022 (S.I. 444 of 2022), authorise an Irish based telecommunications provider to withhold relevant revenues to its onward telecommunications provider if the calls are the result of fraud or misuse of numbers. ComReg uses this authority with discretion. Where the telecommunications provider promptly provides details concerning the incident, ComReg may intervene. We will take into account factors such as the value of the calls, whether appropriate security measures were in place to prevent the hacking, and whether the incident was reported to the Gardai. If ComReg intervenes, it can mean a significant reduction in the call charges billed to the PBX owner. ComReg will only intervene on the first hacking incident and when the Garda report has been confirmed and Pulse number provided.

How does ComReg become involved?

Telecoms Provider detects malicious calls & blocks further calls

→

Telecoms Provider notifies PBX owner of hacking

→

Telecoms Provider obtains relevant information from PBX owner

→

Telecoms Provider reports hacking to ComReg

→

ComReg reviews the report & may issue a Withhold Revenue Order.

ComReg can only stop revenue flows from hacked calls if it receives the required information before bills are paid by any operator in the chain of handling the call. It is important that PBX owners work together with their telecom's provider. Further information is available at the following link. <https://www.comreg.ie/industry/electronic-communications/compliance-enforcement/misuse/>