# Regulation 23(2) Process

## An Operator's Information Note

Information Notice

**Reference:** ComReg 15/43r

**Version:** Final 1.0

**Date:** 28 January 2016

**An Coimisiún um Rialáil Cumarsáide**
**Commission for Communications Regulation**
Abbey Court Irish Life Centre Lower Abbey Street Dublin 1 Ireland
Telephone +353 1 804 9600 Fax +353 1 804 9680 Email info@comreg.ie Web www.comreg.ie

## Additional Information

| | |
|---|---|
| Document No: | 15/43r |
| Date: | 28 January 2016 |

# Content

## Section Page

# Annex

## Section Page

# 1 Introduction

1. In 2011, an amended version of Article 28(2) of the Universal Service Directive[1] came into force, the revised provision of which related to end-user protection in the case of fraud or misuse. The amended Article 28(2) established 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 of misuse and to require that in such cases providers of electronic communications services withhold relevant interconnection and other service revenues".

2. 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) 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.*"

3. The "Regulator" for these purposes is the Commission for Communications Regulation ("ComReg").[2]

4. This information note describes ComReg's policy and process in respect of a decision to utilise Regulation 23(2) in a case of misuse (most often in the form of a Private Branch Exchange ("PBX") hack).

5. It should be noted that both the policy and process are guidelines which would normally be followed but that this policy and process are not binding on ComReg and alternative approaches may be used depending on the circumstances of the individual case.

[1] Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (the "Universal Service Directive") as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (the "Citizens' Rights Directive").

[2] See Regulation 2 of the European Communities (Electronic Communications Networks and Services) (Framework) Regulations 2011 (the "Framework Regulations") and Regulation 2 of the Universal Service Regulations.

6. The incidents which require the use of Regulation 23(2) are often cross border in nature and include operators in a number of Member States and countries outside the EU. Consequently, Guidelines for co-operation between Member States in relation to Article 28(2) have been provided by BEREC in its paper "Article 28(2) USD Universal Service Directive: A harmonised BEREC cooperation process" (the "BEREC Guidance")[3] ComReg's policy and process in respect of Regulation 23(2) is informed by the BEREC Guidance.

[3] Document number: BoR (13) 37 Document date: 07.03.2013

# 2 Executive Summary

7. The main focus of ComReg's intervention in misuse cases is end-user protection. In deciding whether an incident constitutes a fraud or misuse within the meaning of Regulation 23(2), ComReg will be guided by the BEREC Guidance Paper[4]. As noted in paragraph 1 of that guidance, "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…". The examples provided are as follows[5]:

    a. Use of numbering intended for an end-user for the provision of services not included in the national numbering plan of the relevant jurisdiction (for example auto-dialling)

    b. The use of an unallocated number by a party without the consent of the allocating entity (for example 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 part to whom it was allocated (for example phone hijacking, or PBX hijacking)

    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.

8. The majority of incidents that are brought to ComReg's attention relate to PBX hacking. This type of incident would typically involve a third party hacking into a business telephone system (PBX) and causing high volumes of calls to be made to high termination rate international destinations. The motivation for this is that the fraudster will receive a payment for the calls being terminated on these numbers.

[4] BEREC Guidance Paper on Article 28(2) Universal Services Directive of 7th March 2013 which can be found at the following link: 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

[5] At paragraph 54, BEREC Guidance Paper on Article 28(2) Universal Services Directive of 7th March 2013.

9. ComReg aims to protect the Irish end-user from financial loss that is associated with misuse as described in BEREC document BoR(13)37 and also to deter potential perpetrators of fraud and/or misuse by disrupting the flow of revenue to such activities and thereby making such activities less profitable and so less attractive.[6] ComReg also aims to raise awareness among end-users and operators with a view to enhancing protection measures by these parties.[7] With these ends in mind, ComReg has developed a process for dealing with reported incidents of misuse.

10. This information note provides some detail on the process used by ComReg for such reported incidents.

11. The process relies heavily on timely reporting of incidents by operators and end-users and the timely provision of information by operators to ComReg. Delays in the provision of information can lead to end users or operators that are slow to respond being left with significant costs that cannot be recovered.

12. Timely reporting of suspected incidents of fraud/misuse is essential because when international calls are made there are payments made between all the operators involved in the delivery of the calls. Typically there will be several such operators for a single international call. International processes typically involve the payments for the calls being made from 4 to 8 weeks after the call is made. Hence, ComReg's intervention is typically limited to intervening in this period.

13. If ComReg decides to intervene in an incident, it will do so initially with an interim order requiring the affected operator(s) to withhold interconnection revenues and associated service revenues of the relevant calls (and, where appropriate, to block access to relevant numbers or services) for a period of four months.[8] Following an investigation by ComReg into the circumstances of the incident and having considered any representations by interested parties, if after the interim period ComReg is still of the opinion that fraud or misuse of an Irish number has occurred, the interim requirement may be made permanent.

14. 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 taken in respect of their equipment. ComReg judges each case on its merits when deciding whether or not to intervene.

15. Regular monitoring of traffic by operators, in particular to high cost destinations or known high risk destinations, should facilitate early detection of anomalous traffic that is crossing an operator's network and reduce the financial impact of incidents for both operators and end users.

[6] See in this regard paragraphs 20-21 of the BEREC Guidance.
[7] See in this regard paragraph 22 and paragraphs 214-219 of the BEREC Guidance.
[8] See in this regard paragraph 169 of the BEREC Guidance.

16. ComReg would encourage retail operators to ensure that their customers are aware of the risks of misuse of their PBX and similar systems and encourage customers to take appropriate security precautions to reduce their risk of a hack.

# 3 Objective of the process

17. Where ComReg decides to utilise its Regulation 23(2) power when an incident is reported, it will be primarily for the purpose of protection of the end-user of electronic communications services whether a natural person or company (the "End-User"). In the short term, the aim is to reduce End-User and, in some circumstances, operator exposure to fraud or misuse. In addition, the aim is to disrupt the money flow to people or entities which perpetrate fraud or misuse and it is hoped that ComReg's actions, with the assistance of industry using a coordinated approach as defined in the BEREC Article 28(2) process, will disincentivise such incidents in the future.

18. Contract clauses for inter-operator payments associated with fraudulent traffic can result in difficulties for operators seeking to recover costs associated with such traffic where payments have occurred. ComReg would recommend that operators review these inter-operator contracts so that the charges for traffic associated with activity of this nature can be stopped and/or reimbursed. Such changes may negate the requirement for a regulatory intervention in the future and could assist with the disruption of money flows to perpetrators of fraud or misuse.

19. It should be noted that it would be impractical for ComReg to intervene in all incidents, and as suggested in the BEREC Guidelines, consideration will be given to a number of factors, including the impact of the incident (financial or otherwise), when considering whether to intervene. As such ComReg will consider, on a case by case basis, whether the use of Regulation 23(2) is justified.

# 4 Important Points

20. In making a decision to use its Regulation 23(2) power ComReg will consider among other things[9] the following points:

## 4.1 Timeliness of Reporting

21. A delay in notification of an alleged incident by an affected party or a delay in the furnishing of requested details may have adverse consequences with regard to ComReg's ability to investigate and make a decision on the exercise of its power under Regulation 23(2).

22. A report of a PBX hack or any other AIT incident should be brought to ComReg's attention within days of the incident. This is required because of the interconnection payment cycles. ComReg's intervention is aimed at facilitating the disruption of money flows to the person involved in the misuse as well as protection of the end user. The effectiveness of the ComReg intervention may be negatively impacted by delayed reports.

23. It should be noted that the inability to stop all payments in the interconnect payment chain would be not be a sufficient reason to preclude intervention by ComReg, but any unnecessary reporting delays will be considered when deciding on intervention. ComReg will consider each case on its merits.

## 4.2 Whether the End-User has made a complaint to An Garda Síochána

24. Following an incident, the End-User should immediately contact the Gardai to make a formal complaint.[10]

25. A PULSE number should be obtained in all cases.

26. A failure to report a matter to the Gardaí will generally result in ComReg not taking action in respect of a reported incident.

## 4.3 Whether the End-User has experienced previous incidents of misuse

27. ComReg may decide not to intervene in circumstances where the End-User was aware of risks or inadequacies in their security systems but failed to remedy such inadequacies so as to prevent or mitigate against any further misuse or fraud. In particular, ComReg will normally not take a case if an end user has had a previous incident and failed to take remedial action by applying adequate security measures to its telecommunication systems.[11]

[9] Repetition of an incident, appropriate security etc
[10] See paragraph 231 of the BEREC Guidance Paper.
[11] See in this regard paragraph 217-218 of the BEREC Guidance Paper.

## 4.4 End-User protection

28. The primary focus of ComReg's process is to protect the end-user from the consequences of fraud or misuse. This protection is provided directly by intervention with the retail operator, with ComReg requiring interconnection or other service revenues to be withheld.

29. ComReg will also consider intervention which aims to act as a disincentive to future cases of fraud or misuse. This will normally be through attempting to disrupt money flows through the interconnection chain, to the extent that is within ComReg's power, and to provide information to other appropriate bodies to facilitate investigations of cases.[12]ComReg will continue to work and liaise with other NRAs as per the harmonised BEREC cooperation process for Article 28(2) of the Universal Service Directive.

30. When forming a view as to whether to intervene in a particular incident affecting an end user ComReg will consider the operator's intended approach to the retail charge to the end user.

[12] See paragraphs 183 and 190 of the BEREC Guidance Paper.

# 5 Incentives & Recommendations

## 5.1 Operator

31. Operators should monitor traffic passing through their networks to detect any anomalous traffic patterns. A robust detection system should minimise the impact of misuse on end-users .[13]

32. In the event of an incident being identified by an operator, the end user should be advised immediately to assess the issue.

33. When an incident is confirmed, ComReg should be advised immediately of the details of the incident. ComReg will need to know that the incident has stopped and will require details of calls such as:

    a. the originating number(s),

    b. the terminating number(s),

    c. call time(s),

    d. call duration(s) and

    e. the route(s) the call(s) used

    f. along with the appropriate contact details for the next relevant operator in the chain.

34. It should be noted that if a hack occurs an operator may be left liable for all or part of the bill if ComReg decides not to intervene in the case. It should be remembered that ComReg reviews each case on its merits and in the majority of cases, ComReg does not intervene.

35. Operators should regularly provide briefing material for their business customers outlining the risks and suggesting preventative measures.[14]

## 5.2 End-user

36. The two most significant factors affecting an end-user are financial loss and a potential disruption to its business through barring of calls. A business can protect itself from this by ensuring its PBX is properly secured to guard against a hack or other misuse by unauthorised third parties.[15]

37. The incentive for the end-user to secure a system is to reduce the risk of excessive bills for unauthorised traffic

[13] See paragraphs 220-222 of the BEREC Guidance Paper.
[14] See paragraph 219 of the BEREC Guidance Paper.
[15] See paragraphs 217-218 of the BEREC Guidance Paper.

38. It should be remembered that ComReg reviews each case on its merits and will not automatically intervene in a case. Therefore, it is important for an end-user to take reasonable steps to protect themselves from hacking or other forms of misuse.

39. If an end-user suspects that it may be a victim of such a crime, it should contact its local Garda station and make a formal complaint, contact ComReg as quickly as possible, and contact its PBX maintainer to upgrade its security settings and block relevant calls immediately.

# 6 The ComReg Process for Investigating Regulation23(2) cases

## 6.1 Case initiation

40. ComReg is notified of an issue.

41. To report an incident to ComReg please email us at misuse@comreg.ie

42. ComReg will assess the notified issue.

43. An initial review is held to determine if it is recommended to accept or reject the case.

## 6.2 Initial investigation

44. ComReg will require that the "Fraud or Misuse Notification Form" (attached at Appendix 1 hereto) be completed by the End-User and/or Primary Operator.

45. If the end-user fails (or chooses not) to contact ComReg after ComReg seeks information about the hack then ComReg may decline to intervene in the case.

46. ComReg will request relevant information from the retail operator involved or other operators in the chain which have been identified as providing interconnection services relating to the fraud or misuse.

47. Operators know that ComReg is working to a tight timeline and so it is expected that operators will provide information and report an incident to ComReg in a timely manner.

## 6.3 Notification of initial decision

48. In the event that it is decided not to utilise the Regulation 23(2) legislation, ComReg notifies the relevant operators.

49. In the event that it is decided to utilise the Regulation 23(2) legislation, ComReg notifies, by way of letter, the relevant operator(s) of the decision to utilise the Regulation 23(2) legislation.

50. The 4 month interim window commences on the date the letter to the retail operator is issued.

## 6.4 Continuing investigation during the Interim Period

51. ComReg notifies other operators of the investigation and asks them to provide information in relation to the Relevant Calls. If ComReg identifies that the Relevant Calls appear to be destined to terminate in another European Union Member State it will notify the NRA in the relevant country and advise it of the investigation and decision. Where the calls appear to terminate in a country outside the European Union, ComReg will, where practical, contact the appropriate body in that country and co-ordinate with them to the extent it considers appropriate on a case-by-case basis.

## 6.5 Decision on whether to issue a permanent Regulation 23(2) requirement

52. Following receipt of any representations made by interested parties, but no later than 4 months after the interim Regulation 23(2) requirement is made, ComReg will decide whether or not to confirm the provisional finding of fraud or misuse and make the interim Regulation 23(2) requirement permanent.

## 6.6 Notification of final decision

53. ComReg formally notifies the Primary Operator and/or other Operators of the decision made at paragraph 52.

## 6.7 Change to the process

54. The process set out above is subject to change depending on the circumstances of each individual case. The process itself may be changed from time to time by ComReg if it is considered necessary.

# Annex: 1 Misuse Notification Form

## Operator Misuse Notification Form

**Please complete the form fully and return to ComReg no later than 3 working days after receipt**

**Failure to complete the form or return it in a timely manner may mean that ComReg may decide not to take action in relation to your case. Additionally ComReg may use its formal powers to request information if considered necessary**

**(Please overtype explanation in italics)**

| | |
|---|---|
| **End User Name** | *Name of Company or consumer* |
| **End User Contact Name** | *Please provide an End User contact name.* |
| **End User Contact Phone Number** | |
| **End User Contact e-mail** | |
| **End User Contact Address** | |
| **Name of operator (1) providing service** | *Operator Name* |
| **Operator Contact Name** | |
| **Operator Contact e-mail** | |
| **Operator Contact Address** | |
| **Operator Contact Phone No** | |
| **Account Number** | *Customer account no* |
| **Typical size of equivalent monthly bill** | *Please provide an estimate of the End User's average monthly bill* |
| **Garda Reference Number** | *Incidents of misuse must be notified by the End User to the Gardai at any local Garda station. Please provide the PULSE number or reference from local Garda station and name of Garda taking the complaint.* |

| | |
|---|---|
| **Description of the incident** | *Description of the incident including:*<br>• *Date and Time of incident start and end;*<br>• *Destination of calls;*<br>• *Circumstances causing the incident;*<br>• *How the incident was identified;*<br>• *Detail any remedial action put in place;*<br>• *Detail whether the problem is ongoing or has stopped;*<br>• *PBX type when calls were routed through a PBX;*<br>• *Location of the PBX.*<br>• *Who owns of the PBX*<br>• *Who is responsible for the PBX security/maintenance*<br>• *Confirmation that the relevant number was allocated to the End-User;*<br>• *Verification that an internal review has been conducted i.e. that the alleged fraud or misuse was carried without the consent of the person to whom the number was allocated;*<br>• *Contact details for other significant people, such as PBX maintainers* |
| **Call Detail Record (CDR) to be provided by retail operator** | *If available on excel spread sheet or similar please provide in this format. (Operators must attach the relevant CDRs).*<br>*(a) A-Number*<br>*(b) B-Number*<br>*(c) Date/Time of call (dd/mm/yy hh:mm:ss)*<br>*(d) Duration of call (hh:mm:ss)*<br>*(e) Interconnect carrier*<br>*(f) Retail Cost of call*<br>*(g) Wholesale Cost of call*<br>*Only calls relevant to the incident should be included.* |
| **Name of Interconnect Carrier(s)**<br>**Were the calls handed over to the interconnect operator(s) in the republic of Ireland?** | *Yes/No* |

| | |
|---|---|
| **If the calls were handed over outside the Republic of Ireland, where were they handed over?** | *Name of country* |
| **Estimated Retail value of Calls to be provided by retail operator** | *Please provide an estimated Retail value of the calls from the incident.* |
| **Estimated wholesale value of Calls to be provided by retail operator** | *Please provide an estimated wholesale value of the calls from the incident.* |
| **Billing Operator** | *Please provide the name of the operator responsible for billing the End User.* |
| **Interconnect Payment Date to be provided by retail operator** | *Please provide the date for payment(s) to interconnection operator(s)* |
| **End-User Bill Date to be provided by retail operator** | *Please indicate the date on which the end user is due to receive a bill for the calls resulting from the incident and the payment due date.* |
| **If ComReg intervenes and stops wholesale payments will operator waive all charges to the customer for the relevant calls?** | *Yes/No* |
| **If ComReg does not intervene will operator charge the customer wholesale rates only for the relevant calls?** | *Yes/No* |