Confirmation Decision under section 96C of the Communications Act 2003 relating to Contravention of General Condition 3.1(c)

Confirmation Decision served on Hutchison 3G UK Limited by the Office of Communications

This version is non-confidential
Confidential redactions are indicated by [✂]

Issue date: 16 June 2017

Contents

Glossary of terms

Act – the Communications Act 2003.

Affected Area – Kent, Hampshire, and South-East London, including central London.

[✂] – [✂].

[✂APN – Affected Part of Three's Network] which connects [✂Data Centre 1] and [✂Data Centre 2] to various other sites at which call traffic is interconnected.

CP – Communications Provider.

CHA – Call Handling Agents for emergency calls.

[✂Data Centre 1] and [✂Data Centre 2] – Three's data centres located in [✂]. These sites process traffic for customers connected to Three's RAN in the Affected Area.

[✂Data Centre 3] – the data centre building known as [✂Data Centre 3] operated by [✂THIRD PARTY1], through which Emergency Call Traffic is routed to BT.

EC-RRG Resilience Guidelines – Electronic Communications Resilience & Response Group Resilience *"Guidelines for Providers of Critical National Telecommunications Infrastructure"*, March 2008.

Emergency Call Service(s) – the service that Three provides to Three Customers hosted by [✂Data Centre 1] and [✂Data Centre 2] to enable them to access emergency organisations by using the emergency call numbers "112" and "999".

Emergency Call Traffic – calls to the emergency call numbers "999" and "112" which originate on the portion of Three's RAN in the Affected Area.

Fibre Break #1 – the fibre break which took place on the [✂APN] between [✂Data Centre 1] and [✂Data Centre 3] at [✂] on [✂] October 2016.

Fibre Break #2 – the fibre break which took place on the [✂APN] between [✂Data Centre 2] and [✂Data Centre 3] at [✂] on [✂] October 2016.

First S135 Notice – the notice, issued by Ofcom on 12 December 2016, requiring the provision of specified information under section 135 of the Act.

General Conditions of Entitlement – General conditions, imposed under section 45 of the Act, which apply to all persons providing electronic communications networks and services.[1]

Incident – the loss of the Emergency Call Service which took place between the time that Fibre Break #2 took place and the time that the Emergency Call Service was fully restored.

Incident Report – the report provided by Three to Ofcom on 6 October 2016 pursuant to section 105B of the Communications Act 2003.

Interim Solution – alternative transmission route put in place by Three [✂] on 6 October 2016 enabling emergency calls to bypass the [✂APN] by routing Emergency Call Traffic to pre-existing handover points on Three's core network.

[1] A consolidated version of the General Conditions of entitlement is available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0026/86273/CONSOLIDATED_VERSION_OF_GENERAL_CONDITIONS_AS_AT_28_MAY_2015-1.pdf

MBNL – Mobile Broadband Network Ltd, an infrastructure sharing joint venture between EE and Three relating to the RAN.

MNO – Mobile Network Operator.

PECN – Public Electronic Communications Networks: an electronic communications network provided wholly or mainly for the purpose of making electronic communications services available to members of the public.[2]

PCN – Public Communications Network: an Electronic Communications Network used wholly or mainly for the provision of Public Electronic Communications Services which support the transfer of information between Network Termination Points.[3]

Penalty Guidelines – Ofcom's published guidelines dated 3 December 2015 which set out how Ofcom proposes to determine the amount of the penalties which it imposes.[4]

Period of Infringement – 26 May 2011 up to [✂] on 6 October 2016.

RAN – Radio Access Network; the part of mobile telecommunications network that manages the wireless connections between end-user devices and the rest of the network.

Second S135 Notice – the notice requiring the provision of specified information under section 135 of the Act issued by Ofcom on 1 February 2017.

[✂Third Party 1] – [✂].

[✂Third Party 2] – [✂].

Third S135 Notice – the notice, issued by Ofcom on 8 March 2017, requiring the provision of specified information under section 135 of the Act.

Three Core Network – the rest of Three's core network other than the [✂APN].

Three's RAN – the portion of the Three/MBNL Radio Access Network supported by [✂Data Centre 1] and [✂Data Centre 2], which provides connectivity to customers in the Affected Area.

[2] Definition from section 151(1) of the Act.
[3] Definition set out in Ofcom's *"Changes to General Conditions and Universal Service Conditions",* Statement dated 25 May 2011.
[4] *"Ofcom Penalty Guidelines. S.392 Communications Act 2003"*, Guidelines, 3 December 2015. Available at http://www.ofcom.org.uk/content/about/policies-guidelines/penality/Penalty_guidelines_2015.pdf.

Section 1

Executive Summary

1.1 This document (the "Explanatory Statement") explains Ofcom's reasons for giving Hutchison 3G UK Ltd ("Three") a confirmation decision (the "Confirmation Decision") under section 96C of the Communications Act 2003 (the "Act") in respect of its contravention of General Condition 3.1(c) of the General Conditions of Entitlement ("GC3.1(c)"). The Confirmation Decision itself is at Annex 1.

1.2 GC3.1(c) requires communications providers ("CPs") to take all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations as part of any publicly available telephone service offered.

1.3 Ofcom has determined that Three contravened GC3.1(c) during the period 26 May 2011 to 6 October 2016 (the "Period of Infringement")[5] and has imposed a penalty of £1.89 million in respect of Three's contravention. The Confirmation Decision sets out Ofcom's determination, including the amount of the penalty and the steps Three is required to take to ensure it complies with the requirements of GC3.1(c).

1.4 The particularly high standard imposed by GC3.1(c) reflects the fact that telephone access to emergency organisations is of utmost importance to public health and security. As such, Ofcom expects CPs to have done everything they possibly can to ensure that their customers have uninterrupted telephone access to emergency organisations. In particular, CPs should ensure that their networks and services are resilient, including, as reflected in industry best practice, avoiding single points of failure wherever possible.

1.5 On 6 October 2016, Three notified Ofcom of an incident, caused by a double fibre break on the [✂] ("[✂APN]"), which had resulted in a temporary loss of service to Three's customers in Kent, Hampshire, and South-East London, including central London (the "Affected Area").[6] The loss of service included failure to connect 999 and 112 calls to emergency organisations between [✂] and [✂] (the "Incident").

1.6 As all emergency calls in the Affected Area were routed through [✂] ("[✂Data Centre 3]") and the double fibre break isolated [✂Data Centre 3] from the rest of the network, Three was, during the Incident, unable to convey emergency calls originating from Three's customers in the Affected Area ("Emergency Call Traffic") to its normal interconnect points with BT for onward transmission to BT Call Handling Agents for emergency calls ("CHAs"). The Incident was resolved by introducing an additional route that did not convey Emergency Call Traffic via the [✂APN] and [✂Data Centre 3].

[5] Emergency Call Traffic had been routed in the same way for the entirety of the period during which GC3.1 has applied to Three. See Section 2, paragraph 2.5.
[6] Section 105B of the Act requires CPs to notify a breach of security which has a significant impact on the operation of the network or service or a reduction in the availability of the network which has a significant impact on the network. See Section 2, paragraph 2.11.

1.7 We opened an investigation on 28 November 2016 into whether there was or had been a contravention of Three's obligations under GC3.1 and/or section 105A(1)-(3) of the Act (the "Investigation").[7]

1.8 The Incident highlighted that all pre-configured routes for Emergency Call Traffic to reach BT interconnect points appeared to rely on a single building, [✂Data Centre 3]. This raised a concern about the resilience of its network and its compliance with the requirements of GC3.1(c).

1.9 Based on the evidence received during the Investigation, Ofcom considered that there were reasonable grounds for believing that Three had contravened GC3.1(c) during the Period of Infringement by failing to meet the high standard imposed on CPs in GC3.1(c) to take all necessary measures to maintain, to the greatest extent possible, uninterrupted telephone access to emergency organisations. Accordingly, on 2 June 2017, we issued Three with a notification under section 96A of the Act (the "S96A Notification").

1.10 The S96A Notification set out Ofcom's provisional finding that Three had contravened GC3.1(c) and that Ofcom was minded to impose a penalty and to require Three to take specified steps, to the extent it has not already taken them, to ensure it complies with the requirements of GC3.1(c). The S96A Notification also gave Three the opportunity to make written and/or oral representations on the notified matters.

1.11 On 9 June 2017, Three wrote to Ofcom as part of the voluntary settlement procedure it had entered into with Ofcom:

- admitting it had contravened GC3.1(c) in the period 26 May 2011 to 6 October 2016, as set out in the S96A Notification;
- accepting a streamlined administrative process to conclude this matter;
- confirming that it would pay the penalty set by Ofcom, recognising that because of its admission, the penalty would be reduced in the Confirmation Decision; and
- accepting the steps it is required to take to ensure compliance with the requirements of GC3.1(c) and that the reduction in penalty is conditional on Three taking those steps.

1.12 Based on the information and evidence referred to above, and the admissions Three has made, Ofcom is satisfied that Three contravened GC3.1(c) during the Period of Infringement for the following reasons:

1.12.1 Three failed to ensure sufficient resilience in its network as it was routing all Emergency Call Traffic through one single location ([✂Data Centre 3]) thereby leaving the service vulnerable to a single point of failure;

1.12.2 there were no alternative routes pre-configured on Three's network which, in the event [✂Data Centre 3] was unavailable, would allow Emergency Call Traffic to be automatically re-routed to BT interconnect points without interruption to service; and

[7] Section 105A of the Act requires providers of public electronic communications networks and services to take technical and organisational measures appropriately to manage risks to the security of their networks and services.

1.12.3 it would have been technically feasible and within Three's reasonable control to have sufficient resilience in the provision of its Emergency Call Service.

1.13 In the light of our findings in relation to GC3.1(c) we do not consider it necessary to also consider whether Three has contravened section 105A of the Act.

1.14 As part of ensuring it takes all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations, Three is required to take the following steps, to the extent it has not already taken them:

1.14.1 to ensure that the routing of its Emergency Call Traffic is sufficiently resilient (as described in this document); and

1.14.2 to put in place processes for ongoing review and management of the risk associated with the conveyance of its Emergency Call Traffic, and to provide Ofcom with a description of how this ongoing review and management of risks is to be conducted.

1.15 We have determined that a penalty of £1.89 million is appropriate and proportionate to the contravention in respect of which it is imposed. In taking this view, we have had regard to the evidence referred to in Sections 2, 3, 4, 5 and Annex 2 of this document, together with Ofcom's Penalty Guidelines.[8] The basis for Ofcom's view as to the amount of the penalty is explained in Section 6.

1.16 The above amount includes a 30% reduction to the proposed penalty set out in the S96A Notification, as a result of Three accepting liability and entering into a voluntary settlement with Ofcom. This reflects the cooperation offered by Three during the investigation and the resource savings resulting from its acceptance of a streamlined administrative process.

[8] *"Ofcom Penalty Guidelines. S.392 Communications Act 2003"*, Guidelines, 3 December 2015. Available at http://www.ofcom.org.uk/content/about/policies-guidelines/penality/Penalty_guidelines_2015.pdf.

Section 2

Regulatory Framework

Introduction

2.1 This section sets out the legal framework that is relevant to the Investigation. It looks at the regulatory obligations that apply to CPs specifically in relation to the provision of uninterrupted access to emergency organisations and those relating to the security of electronic communications networks and services more generally. It then sets out the focus of Ofcom's investigation in this case and our investigation and enforcement powers.

General Condition GC3.1

2.2 The General Conditions of Entitlement impose specific obligations on CPs offering publicly available telephone services in relation to the provision of access to emergency organisations. These obligations, set out in GC3.1(c) and General Condition 4 (GC4), are extensive because of the critical nature of telephone access to the emergency organisations.

2.3 GC3.1, the relevant obligation for the purposes of the Investigation, requires that:

> *"The Communications Provider shall take all necessary measures to maintain, to the greatest extent possible:*
>
> a) *the proper and effective functioning of the Public Communications Network provided by it at all times, and*
>
> b) *in the event of catastrophic network breakdown or in cases of force majeure the fullest possible availability of the Public Communications Network and Publicly Available Telephone Services provided by it, and*
>
> c) *uninterrupted access to Emergency Organisations as part of any Publicly Available Telephone Services offered."*[9]

2.4 GC3.1 implements Article 23 of the Universal Service Directive[10] which stipulates that "*Member States shall take all necessary measures to ensure the fullest possible availability of publicly available telephone services provided over public communications networks in the event of catastrophic network breakdown or in cases of force majeure. Member States shall ensure that undertakings providing publicly available telephone services take all necessary measures to ensure uninterrupted access to emergency services.*"

[9] A consolidated version of the General Conditions is available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0026/86273/CONSOLIDATED_VERSION_OF_GENERAL_CONDITIONS_AS_AT_28_MAY_2015-1.pdf.

[10] "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…". See: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&from=EN

2.5 GC3.1 has applied in its current form to all providers of Public Communications Networks ("PCNs") and telephony services since 26 May 2011 following changes to the underlying EU framework.[11] From 26 May 2011, GC3.1 has applied to mobile networks and service providers in addition to fixed network and service providers (previously, GC3.1 applied only to fixed networks and services).

Sections 105A and 105B

2.6 In addition to the specific provisions set out above in relation to the provision of access to emergency call services, sections 105A to 105D of the Act contain general provisions in relation to the security of public electronic communications networks ("PECN") and services. These provisions were introduced into the Act by the Electronic Communications and Wireless Telegraphy Regulations 2011, as part of the amendments made to implement changes to the European Regulatory Framework[12] and took effect from 26 May 2011.[13]

2.7 Section 105A(1) imposes an obligation on CPs to take technical and organisational measures to appropriately manage risks to the security of public electronic communications networks and services. According to section 105A(2), such measures should include, in particular, measures to prevent or minimise the impact of security incidents on end-users. These provisions of the Act implement paragraph 1 of Article 13a of the Framework Directive which requires Member States to ensure that:

> *"undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services. Having regard to the state of the art, these measures shall ensure a level of security appropriate to the risk presented. In particular, measures shall be taken to prevent and minimise the impact of security incidents on users and interconnected networks."*

2.8 Ofcom has published guidance on the application of section 105A of the Act, initially on 10 May 2011[14] and then again in August 2014.[15] The two sets of guidance do not materially differ in terms of the guidance provided in relation to section 105A. In both

[11] The Framework consists of five Directives: the *Framework Directive* (2002/21/EC), *Authorisation Directive* (2002/20/EC), *Access Directive* (2002/19/EC), *Universal Service Directive* (2002/22/EC), *Privacy and Electronic Communications* (2002/58/EC); all as amended by the *Better Regulation Directive* (2009/140/EC) and *Citizens' Rights Directive* (2009/136/EC).
[12] See paragraphs 4 and 65 of Schedule 1 to the Electronic Communications and Wireless Telegraphy Regulations 2011. See http://www.legislation.gov.uk/uksi/2011/1210/pdfs/uksi_20111210_en.pdf.
[13] SI 2011/1210. Paragraph 65 of Schedule 1 to the Regulations introduced sections 105A-105D into the Act. See http://www.legislation.gov.uk/uksi/2011/1210/pdfs/uksi_20111210_en.pdf.
[14] *Ofcom guidance on security requirements in the revised Communications Act 2003: implementing the revised EU Framework*, 10 May 2011. Ofcom published minor revisions to this guidance on 3 February 2012. See http://webarchive.nationalarchives.gov.uk/20120619191730/http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/security-resilience/guidance.pdf.
[15] *Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003*, 8 August 2014: http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/security-resilience/ofcom-guidance.pdf.

sets of guidance, the meaning of "security" in the context of sections 105A to 105D is defined as "*protecting confidentiality, integrity and availability*".[16]

2.9 The guidance issued in May 2011 makes explicit reference to emergency services. It states that:

> "*In the context of protecting end users, we consider that the protection of access to the emergency services is a special case on which we place particular importance. […] Section 105A(2) places security protection requirements on CPs which are broader than the availability obligations in GC3. When considering compliance with these broader requirements, in the context of CPs offering emergency services access, we will have a higher expectation than for other services. This will be in line with the importance of their role and the obligations under the GCs*."[17]

2.10 The guidance issued in August 2014 also notes that:

> *"[i]n general, network providers should take measures to maintain availability appropriate to the needs of their direct customers. An important exception to this principle is for networks offering public access to the emergency services. For these networks and the services they support, GC3 imposes specific and strict requirements for maintaining availability and will continue to apply".*[18]

2.11 Section 105B of the Act requires CPs to notify a breach of security which has a significant impact on the operation of the network or service or a reduction in the availability of the network which has a significant impact on the network.

Focus of the Investigation

2.12 As follows from the above, the relevant regulatory obligations relating to network availability and access to emergency organisations are in GC3.1(c) and section 105A. However, as also set out in the guidance issued in May 2011 and the guidance issued in August 2014,[19] the obligations in GC3.1(c) are in this context more onerous than those in section 105A because of the critical nature of access to emergency services for end-users.[20] In a situation where access to emergency services has been compromised we will therefore be concerned to ensure that a CP has met these more onerous obligations before any consideration of the broader security protection requirements in section 105A.

---

[16] May 2011 Guidance, paragraph 3.4; August 2014 Guidance, paragraph 3.2.
[17] May 2011 Guidance, paragraph 3.15. The requirements of GC3 are discussed below.
[18] See "*Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003",* 8 August 2014, paragraph 3.33. See: http://stakeholders.ofcom.org.uk/binaries/telecoms/policy/security-resilience/ofcom-guidance.pdf.
[19] See paragraphs 2.9 and 2.10 above.
[20] GC3.1(c) refers specifically to the maintenance of uninterrupted access to emergency organisations as part of the provision of publicly available telephone services, while section 105A requires generally the taking of technical and organisational measures to manage risk to the security of public electronic communications networks and services. GC3.1(c) sets a stricter standard by requiring the taking of "all necessary measures" to ensure uninterrupted access to emergency organisations, compared to the requirement in section 105A of the Act to take measures "appropriately to manage risks".

2.13 Given this, we focused our investigation on Three's compliance with GC3.1(c), during the period from 26 May 2011[21] until 6 October 2016, i.e. the date that the Incident was resolved. Our analysis in Section 5 below reflects this.

2.14 In the light of our conclusions in Section 5, we do not consider it necessary also to assess Three's compliance with section 105A of the Act.

Ofcom's investigation and enforcement powers

2.15 Sections 96A to 96C of the Act set out Ofcom's enforcement powers in cases where we determine there are reasonable grounds for believing that a person is contravening, or has contravened a General Condition of Entitlement.

2.16 Section 96A of the Act provides for Ofcom to issue a notification setting out Ofcom's preliminary view of the alleged contravention. A section 96A notification will include, amongst other things:

a) the steps which Ofcom considers should be taken to comply with the relevant requirement and to remedy the consequences of the contravention;

b) the period within which the subject of the investigation may make representations in response to Ofcom's preliminary views; and

c) details of any penalty that Ofcom is minded to impose for the alleged contravention in accordance with section 96B of the Act.

2.17 Section 96C of the Act provides that, on expiry of the period allowed for representations, Ofcom may either:

a) issue a confirmation decision, confirming the imposition of requirements on the subject of the investigation and the imposition of the penalty specified in the section 96A notification or a lesser penalty; or

b) inform the person we are satisfied with their representations and that no further action will be taken.

[21] As set out in paragraph 2.5 above, GC3.1 has applied to mobile networks and service providers in addition to fixed network and service providers since 26 May 2011 (previously, GC3.1 applied only to fixed networks and services).

Section 3

The Investigation

The decision to investigate

3.1 Network failures are not uncommon. In 2016, Ofcom received 581 incident reports from fixed and mobile CPs under section 105B of the Act. The vast majority of reports were from fixed providers regarding disruption to telephony services (including to emergency organisations) for fewer than 10,000 customers and for less than one day. Incidents with a wider impact are less common.[22]

3.2 Ofcom considers what action to take in respect of each report that it receives, taking into account the circumstances of the particular incident reported. Ofcom will always take particularly seriously notifications by CPs which relate to incidents that adversely affect calls to emergency organisations, due to the potential for significant harm to be caused to citizens and consumers.

3.3 In this case, on 6 October 2016, in accordance with section 105B of the Act, Three notified us of the Incident, which had resulted in voice call failures in the Affected Area. A copy of the incident report is attached at Annex 3. During a call on 19 October 2016 and a subsequent meeting on 2 November 2016, Three confirmed that the Incident resulted in failures of emergency calls.

3.4 Following these discussions, we had initial concerns around the resilience of the routing of Three's Emergency Call Traffic and the potential seriousness and risk to the public caused by a loss of telephone access to emergency organisations.[23] We therefore considered that it was proportionate and appropriate to open a formal investigation in order to assess Three's compliance with GC3.1(c) and/or section 105A(1) to (3) of the Act.[24] The Investigation was opened on 28 November 2016.

Information gathering

3.5 As part of our investigation, we used our powers under section 135 of the Act to gather information from Three. We sent Three a formal request for information under section 135 of the Act on 12 December 2016 (the "First S135 Notice") in relation to the Incident; Three's network configuration; any risk assessments carried out by Three prior to the Incident; and the contingency planning Three had in place relating to the conveyance of Emergency Call Traffic. Three responded in three parts, on 16 December 2016, 16 January 2017 and 18 January 2017 respectively. Copies of these responses are in Annexes 4, 5 and 6.

3.6 On 1 February 2017, we sent a second formal request for information (the "Second S135 Notice") asking for further detail regarding the configuration of the [✂APN] (and, in particular, how Three's network connects with BT interconnect points via [✂Data Centre 3]); the risk assessments Three had carried out; the actions Three took following the Incident; and the interim solution that was implemented. Three

[22] See: Connected Nations report, page 61: https://www.ofcom.org.uk/__data/assets/pdf_file/0035/95876/CN-Report-2016.pdf.
[23] We are currently not aware of any actual harm caused following these failures.
[24] As set out in Section 2, we have focussed our investigation on GC3.1.

responded in three parts, on 15 February, 17 February and 20 February 2017 respectively. Copies of these responses are in Annexes 7, 8 and 9.

3.7 On 8 March 2017, we sent a third formal request for information under section 135 of the Act (the "Third S135 Notice") asking for further information relating to the end to end routing of Emergency Call Traffic through to the London interconnect points with the BT network. Three responded in two parts, on 10 March 2017 and 15 March 2017 respectively. Copies of these responses are in Annexes 10 and 11.

3.8 Three also provided us with a voluntary submission on 15 March 2017. This is included in Annex 12.

Section 4

Relevant facts

Introduction

4.1 This section sets out our understanding of the core factual background relevant to the Investigation and the Incident that took place on [✂] October 2016. More detailed information relevant to our findings is set out in Annex 2.

Access to emergency organisations in the UK

4.2 Telecommunications is a vital part of the national infrastructure. As part of this, access to emergency organisations is of critical importance to public health and security. This is recognised by the UK's statutory and regulatory framework.

4.3 In the UK, a person may make an emergency call, free of charge, using the national telephone numbers 999 or 112. To connect the caller with the correct local emergency service, the call is first answered by an emergency CHA who is able to forward the call to the correct emergency service at the nearest geographic location to the caller, using information provided from the network and from speaking directly to the caller.

4.4 Historically, some CPs provided their own CHA function, but today all CPs purchase CHA services from BT. This means that where CPs have a network of their own, they need to interconnect with the BT network so that emergency calls can be onward routed to BT's CHA services. CPs interconnect with BT for this purpose at locations across the country, at which point emergency calls are handed over to BT to deliver to its CHA centres in the UK.

Three

4.5 Hutchison 3G UK Limited (known under the brand name Three), is an indirectly wholly owned subsidiary of CK Hutchison Holdings Limited ("CKHH") – a limited liability Cayman Islands company registered and listed in Hong Kong. As such, Hutchison 3G UK Limited does not prepare consolidated financial statements and is included in the consolidation of CKHH.[25]

4.6 Three operates a PCN covering 98% of the UK population as well as a publicly available telephone service, providing a mobile communications service which enables access to emergency organisations.[26]

Three's Emergency Call Service for London and the South-East

4.7 Three's network consists of [✂]: [✂]("Core Network") and the [✂APN].[27] When a customer makes a call using the Three network it first gets picked up by the radio

[25] The full Annual Report for 2015 is available at: http://www.ckh.com.hk/en/ir/annual.php and the "Report and Financial Statements" up to 31 December 2015 for Hutchison 3GUK (trading as Three) are available at: https://beta.companieshouse.gov.uk/company/03885486/filing-history.
[26] See Three's website at http://www.three.co.uk/Discover/Network.
[27] The [✂APN] comprises a [✂] connecting [✂] data centres ([✂including Data Centre 1, Data Centre 2 and Data Centre 3]).

access network ("RAN") run by Mobile Broadband Network Ltd ("MBNL") and enters the Core Network at various locations throughout the country.

4.8 During normal operation, calls from customers based in the Affected Area are routed through the [✂APN] to the appropriate part of the network depending on traffic type and call destination.

4.9 Prior to the Incident, Emergency Call Traffic was routed via [✂Data Centre 3] in order to reach interconnect points with BT. [✂] primary and back-up routes [✂were] available, all of which travelled [✂through Data Centre 3], before exiting on one of [✂] possible fibres, each of which connected to a different BT building at which Emergency Call Traffic could be interconnected with the BT network for onward transmission to BT CHAs.

4.10 We understand that for Emergency Call Traffic, routes were available [✂on] the [✂APN]. This configuration allowed traffic to continue to reach [✂Data Centre 3] and the BT interconnect points beyond in the event there was a physical break in the fibre [✂]. In this situation, routes passing through the unaffected part [✂] would automatically be used.

4.11 As stated, Ofcom understands that prior to the Incident all available routes for Emergency Call Traffic passed through one single location ([✂Data Centre 3]). [✂Data Centre 3] has various resilience measures in place relating to site security, power supply, cooling, separation of transmission paths and separation of duct entry points.[28]

4.12 Three's network configuration for Emergency Call Traffic has been in place since [✂ before 2011][29] and Three did not make any changes in 2011 (when mobile operators became subject to GC3.1(c).[30]

The Incident

4.13 The Incident was caused by two fibre breaks on the [✂APN]:

4.13.1 At [✂] October 2016, a [✂] caused a fibre break on the [✂APN] ("Fibre Break #1"). However, as the [✂APN] is [✂], calls could continue to be routed through the [✂APN].[31] Therefore, at this point in time, "*all emergency traffic was routed successfully and the Three network maintained all interconnects to BT in the London area.*"[32]

4.13.2 At [✂] on [✂] October 2016, a second break occurred on a fibre located in a shared maintenance access route ("Fibre Break #2"). Three believes the fibre was accidentally damaged whilst maintenance was carried out on other services by third parties.[33]

[28] See Annex 2, paragraphs A2.13 to A2.17.
[29] Three's response to question 8 of the First S135 Notice, 16 January 2017.
[30] Three's response to question 5a of the Second S135 Notice, 20 February 2017.
[31] A [✂] owned by [✂Third Party 3] caused a fibre break in Three's network. However, Three were able to route emergency calls between [✂Data Centre 1] and [✂Data Centre 3] (via [✂]) following Fibre Break # 1.
[32] Three's response to question 2a of the First S135 Notice,16 January 2017, page 2.
[33] Introduction to Three's response to the First S135 Notice,18 January 2017, page 3.

4.14 Together, Fibre Break #1 and Fibre Break #2, which were at different points on the [✂APN], resulted in all pre-configured routes for Emergency Call Traffic through [✂Data Centre 3] to any of its usual points of interconnect with BT becoming unavailable.[34]

4.15 The Incident resulted in call failures for all Emergency Call Traffic (as defined in paragraph 1.6) from [✂] to [✂].[35] In other words, there was a period of [✂] during which Three's customers in the Affected Area were unable to connect to emergency organisations using the Three mobile network to make calls to 999 and 112 numbers.[36]

4.16 During the Incident, an estimated [✂] customers connected to Three's network (approximately [✂a significant proportion] of Three's active customer base) would have been unable to connect to emergency organisations.[37] As these customers' devices would still have been able to register with Three's network, they would not have been able to take advantage of automatic "emergency roaming" to use an alternative network to make emergency calls. The Incident resulted in [✂] emergency call connection failures from [✂] different customers.[38]

Three's actions in response to the Incident

4.17 Emergency Call Services were restored by Three at [✂] on 6 October 2016 by instituting an additional route for Emergency Call Traffic. This utilised a pre-existing interconnection with BT located elsewhere on Three's Core Network (the "Interim Solution").

4.18 Fibre Break #2 was fully restored at [✂] on 6 October 2016.

Significance of the Incident

4.19 The Incident highlighted that all pre-configured routes for Emergency Call Traffic to reach BT interconnect points appeared to rely on a single building, [✂Data Centre 3]. This raised a concern that [✂Data Centre 3] may represent a "single point of failure" – a point in the network, the failure of which could result in interruption to Three's emergency call service – and in turn brought into question its compliance with the requirements of GC3.1(c).

[34] Information shared with Ofcom in a meeting with Three on 2 November 2016 and confirmed in Three's response to question 1 of the First S135 Notice, dated 16 December 2016, page 2.
[35] The Incident Report, provided to Ofcom on 6 October 2016, suggested that call services were affected from [✂] to [✂] when the fibre break was restored (i.e. [✂]). However, Three subsequently confirmed that its Emergency Call Service was restored [✂] on 6 October 2016. See Three's response to question 1 of the First S135 Notice, 16 December 2016.
[36] Information shared with Ofcom in a meeting with Three on 2 November 2016 and confirmed in Three's response to question 1 of the First S135 Notice, dated 16 December 2016, page 2.
[37] Three's response to question 2b of the First S135 Notice, 16 December 2016, page 3.
[38] Three's response to question 1g of the First S135 Notice, 16 December 2016, page 2.

Section 5

Analysis and evidence of contravention

Introduction

5.1 This section sets out our reasons, including the evidence on which we rely, for concluding that Three has contravened GC3.1(c) by failing to take the necessary measures to maintain, to the greatest extent possible, uninterrupted access to the emergency organisations on 999 and 112 numbers from 26 May 2011 to 6 October 2016.

Summary

5.2 The particularly high standard imposed by GC3.1(c) reflects the fact that telephone access to emergency organisations is of the utmost importance to public health and security. As such, we expect CPs to have done everything they possibly can to ensure that their customers have uninterrupted access to emergency organisations.

5.3 We consider that having sufficient resilience in the provision of emergency call services is an integral element of a CP's obligation to take all necessary measures to maintain uninterrupted access to the emergency organisations as required by GC3.1(c). In particular, we consider that a CP should ensure that there is sufficient diversity in the routing for its emergency calls, including, as reflected in industry best practice, avoiding single points of failure wherever possible.

5.4 We have found that Three's provision of its Emergency Call Service was not sufficiently resilient as:

5.4.1 prior to the Incident, Three routed all Emergency Call Traffic (as defined in paragraph 1.6) through one single location ([✂Data Centre 3]), thereby leaving its Emergency Call Service vulnerable to a single point of failure;

5.4.2 there were no alternative routes pre-configured on Three's network which, in the event [✂Data Centre 3] was unavailable, would allow Emergency Call Traffic to be automatically re-routed to BT interconnect points without interruption to service; and

5.4.3 it would have been technically feasible and within Three's reasonable control to have sufficient resilience in the provision of its Emergency Call Service.

5.5 Consequently, we have concluded that Three failed to meet the requirement to take all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations in contravention of GC3.1(c). The Period of Infringement runs from 26 May 2011[39] until Three introduced an additional routing option for Emergency Call Traffic on 6 October 2016.

5.6 We explain these findings in more detail in the rest of this section.

[39] Since which date Three has been subject to the requirements in GC3.1(c).

Contravention of General Condition 3.1(c)

5.7 GC3.1(c) places an obligation on CPs to take all necessary measures to maintain uninterrupted access to emergency organisations as part of the publicly available telephone services that they offer.

5.8 For the purposes of GC3.1(c),[40] a CP is a person who provides publicly available telephone services. Three provides a mobile telephone service available to members of the public across the UK[41] and is therefore subject to the requirements of GC3.1(c).

Approach to assessing compliance with GC3.1(c)

5.9 Telephone access to the emergency organisations is of critical importance to public health and security. It is for this reason that CPs are required under GC3.1(c) to take *"all necessary measures"* to maintain *"to the greatest extent possible"* uninterrupted access to emergency organisations as part of their publicly available telephone service.

5.10 This obligation sets a particularly high standard for CPs, and clearly recognises the importance of citizens being able to access emergency call services. Therefore, our expectation is that CPs will do everything they possibly can to ensure that citizens have uninterrupted access to the emergency organisations on the 999 and 112 numbers.[42]

5.11 In practice, this is likely to mean CPs having a number of varied measures and contingency plans in place to ensure that they have a resilient emergency call service so that calls to emergency organisations can be routed successfully without risk of an interruption to service. This will require CPs to take particular care when setting up and planning their emergency call services as well as to take active and ongoing steps to ensure that they maintain a sufficient level of resilience.

5.12 When we made changes to the General Conditions in May 2011 (including revising GC3 to reflect changes made to the EU Framework and making mobile operators subject to GC3), some respondents to the consultation sought additional guidance from Ofcom on the interpretation and application of "*all necessary measures*."[43]

5.13 In our 2011 Statement, Ofcom noted that it did not intend, at that time, to issue any general guidance on the application of GC3. We emphasised that it is the responsibility of CPs to whom GC3 applies to consider on the facts and the

[40] See Section 2, paragraph 2.3.
[41] See Section 4, paragraph 4.6 above.
[42] The emergency call numbers, 999 and 112, are fundamental elements of the service: there is an extremely high level of recognition of the numbers by UK citizens and they can be dialled speedily, compared to the eleven digits typically required for the telephone number of a local police or fire station (which the caller is likely to need to look up). Accordingly, we consider that CPs need to provide access to the emergency call numbers of 999 and 112, to the greatest extent possible, in order to meet the obligations in GC3.1(c).
[43] *"Changes to General Conditions and Universal Services Conditions"*, Statement dated 25 May 2011, paragraph 5.10. See:
https://www.ofcom.org.uk/__data/assets/pdf_file/0027/37746/statement.pdf.

circumstances of each case whether they are complying with the obligations imposed by GC3.[44]

5.14 We did, however, clarify in our 2011 Statement that *"[t]o ensure proportionality, any assessment of "all necessary measures" will need to take into account the costs and benefits of maintaining availability in the context of the network or service in question."*[45]

5.15 We also noted[46] that in 2008, industry, via the Electronic Communications Resilience & Response Group ("EC-RRG"),[47] had published guidelines on best practice in the establishment and maintenance of resilience within telecommunications networks and services (the "EC-RRG Resilience Guidelines"), and that these continued to be relevant. According to the EC-RRG Resilience Guidelines:

> "…*the word 'Resilience' is to be interpreted in the broadest sense as the ability of an organisation, resource or structure to be resistant to a range of internal and external threats, to withstand the effects of a partial loss of capability and to recover and resume its provision of service with the minimum reasonable loss of performance*." [48]

5.16 We note that the concepts of resilience and diversity – including the need to avoid potential single points of failure – are well known to the industry. Indeed, their importance is reflected in the EC-RRG Resilience Guidelines, which explicitly state that one of the key risks to resilience is system/logical failures relating to a single point of failure:[49]

> *"To prevent being vulnerable to the failure of a single part of the system, telecommunications companies will invest, where practical, in duplicate or triplicate back-ups for their equipment (redundancy) and diverse transmission routings. Thus the 'logical' architecture of the service will be more resilient than the simple physical layout. But sometimes, due often to human error, these logical configurations can themselves fail to provide the expected level of security. The key is to avoid, wherever possible, 'single points of failure'".*[50]

---

[44] *"Changes to General Conditions and Universal Services Conditions"*, Statement dated 25 May 2011, paragraph 5.12.
[45] *"Changes to General Conditions and Universal Services Conditions"*, Statement dated 25 May 2011, paragraph 5.19.
[46] *"Changes to General Conditions and Universal Services Conditions"*, Statement dated 25 May 2011, paragraph 5.13.
[47] CPs who own or operate key aspects of the telecommunications infrastructure in the UK, including Three, are members of the EC-RRG, see https://www.gov.uk/guidance/telecoms-resilience.
[48] "*EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure",* Guidance March 2008. See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61013/telecoms_ecrrg_resilience_guidelines.pdf, paragraph 2.1.
[49] Other key risks identified in the EC-RRG Guidelines include physical threats, loss of key inputs (such as power failure), software failures and electronic interference. See "*EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure",* March 2008, Paragraph 6.2. See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61013/telecoms_ecrrg_resilience_guidelines.pdf.
[50] "*EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure",* March 2008, paragraph 6.2.3.

5.17 In addition, the EC-RRG Resilience Guidelines specifically state in relation to emergency calls that CPs should:

"*…give particular attention to the security of 999/112 emergency and safety of life traffic, for example by using techniques such as priority routing, repeat attempts, alternative routing and trunk reservation, and by avoiding dependence on a single set of premises for dealing with emergency traffic."*[51]

5.18 Consistent with the above, we consider that having sufficient resilience in the provision of its emergency call service is an integral element of a CP's obligation to maintain uninterrupted access to the emergency organisations as required by GC3.1(c). A key part in enabling this is to ensure that there is sufficient diversity in the routing for emergency calls. Without sufficient diversity in the call routing, a CP's emergency call service will not be resilient and this will put its ability to maintain uninterrupted access to the emergency organisations at unnecessary risk.

5.19 Whilst the ability for a CP to ensure it has 'sufficient diversity' will be constrained by the section of a CP's end to end call routing under consideration, our starting point is that within a CP's core network there should be diversity in the routing of emergency call traffic wherever possible.[52] This is framed by proportionality considerations, which acknowledge that the cost and technology constraints involved in avoiding a single point of failure are likely to vary for different parts of the network. For example, the extent to which diversity can be provided over what is normally referred to as the 'access' network (i.e. between the CP's access node and the customer) is likely to be far more limited than that possible over the rest of a CP's network. Further, where calls leave a CP's own network and are interconnected with others for onwards transmission and handling, the extent to which ensuring sufficient diversity is under the CP's control will likely vary.

5.20 Given this, we have considered the following questions in assessing whether Three has complied with GC3.1(c):

5.20.1 Step 1: Was Three's provision of its Emergency Call Service sufficiently resilient (including considering whether there was diversity in the emergency call routing)?

5.20.2 Step 2: If not, did Three take all necessary steps to ensure that the provision of its Emergency Call Service was sufficiently resilient? In particular, would it have been technically feasible[53] and within Three's reasonable control to ensure sufficient resilience was in place?

5.21 If the answer to the last question is 'Yes', then Ofcom will consider that there has been a breach of Three's obligations under GC3.1(c).

[51] "*EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure",* Guidance March 2008, paragraph 7.1.6 (ii).

[52] In other words, that the network used for emergency call traffic does not rely on a single route, a single point of handover or on routing all such calls or associated signalling traffic through a single location thereby leaving the service vulnerable to a single point of failure, see paragraph 5.23 below.

[53] We consider that what is technically feasible will include an element of proportionality, however this will always need to be considered against the objective of GC3.1(c) – to provide uninterrupted telephone access to the emergency organisations – and the vital public interest that it serves.

Step 1: Was Three's provision of its Emergency Call Service sufficiently resilient?

5.22 As noted above, we consider that one of the most important aspects of ensuring the provision of resilient emergency call services is for a CP to have in place diverse emergency call routing in so far as it is possible and proportionate to do so.

5.23 In particular, we consider that, in line with industry best practice, a CP should ensure that, where possible, the network used for emergency call traffic does not rely on a single route, a single point of handover or on routing emergency calls or associated signalling traffic through one single location, thereby creating vulnerability to a single point of failure. The presence of a potential single point of failure may therefore suggest that there is a lack of diversity and, as such, a lack of resilience within the network (either generally or at specific points within the network).

Three's arguments

5.24 Three has acknowledged the importance of the high standards set out in GC3.1:

"*Three recognises the vital importance of maintaining uninterrupted access to emergency call traffic on its network. Three agrees with Ofcom that the law rightly imposes a strict standard on Communication Providers in this regard".*[54]

5.25 However, Three has submitted that this 'strict standard' is subject to the principle of proportionality, and that it is "*necessary to consider what is properly 'necessary' by way of diversity in network architecture for Three to have maintained 'to the greatest extent possible' the 'uninterrupted access' for emergency calls required by GC3.1(c)."*

5.26 Three also submitted that:

"*…because of the exceptional resilience of [✂Data Centre 3] and Three's equipment connected to [✂Data Centre 3], there was no real risk of [✂Data Centre 3] failing to hand-over Three's emergency call traffic to BT. At all material times there was sufficient diversity in Three's network architecture to safeguard to 'the greatest extent possible' 'uninterrupted access' to emergency calls*." [55]

5.27 Three has further submitted that its Core Network used for Emergency Call Traffic "*does not rely on a single route, location or point of handover*", as "*an alternative route has always been accessible: immediately since October 2016; and prior to that, well within [✂]".*[56]

5.28 Finally, Three has submitted that "*[t]he principles of legal certainty, proportionality and non-discrimination to which Ofcom is subject demonstrate that it would be inappropriate to find Three in breach of GC3.1(c)".*[57] Three appears to make this comment in connection with its view that there was no guidance in this area and that it was *"at all times complying with the relevant industry standards in the absence of specific guidance from Ofcom."*[58] Three goes on to suggest that the appropriate solution would be for Ofcom, should it find industry practice inadequate, to issue

[54] Three's voluntary submission dated 15 March 2017, paragraph 2.
[55] Three's voluntary submission dated 15 March 2017, paragraph 3.
[56] Three's voluntary submission dated 15 March 2017, paragraph 36.
[57] Three's voluntary submission dated 15 March 2017, paragraph 4.
[58] Three's voluntary submission dated 15 March 2017, paragraph 4.

clear guidance and *"contemplate enforcement proceedings such as these only after such guidance is in force".* [59]

5.29 We understand these arguments to be, in essence, that:

5.29.1 Ofcom should not investigate potential contraventions of GC3.1(c) until it has issued relevant guidance on the specific standards required to comply with GC3.1(c);

5.29.2 at the time of the Incident, Three's Emergency Call Service did not, in fact, rely on a single route, location or point of handover and, as such, was diverse and therefore 'sufficiently resilient'; or

5.29.3 even if [✂Data Centre 3] did constitute a single point of failure, it was not 'necessary' to have additional routing in place due to the inherent resilience of Three's network and/or [✂Data Centre 3], meaning that the service was 'sufficiently resilient'. As such, it was not 'necessary' for Three to take further steps to maintain uninterrupted access to emergency organisations within the meaning of GC3.1(c).

5.30 These points are considered in more detail below.

Guidance

5.31 As noted in paragraph 5.13 above, we clearly stated in 2011 that we did not intend to issue guidance on the specific meaning of 'all necessary measures', and that we considered that it is the responsibility of CPs to whom GC3 applies to consider on the facts and circumstances of each case whether they are complying with the obligations imposed therein.[60]

5.32 Moreover, we do not consider that developing such guidance would be a satisfactory alternative to individual enforcement cases which would look in detail at the facts of each individual case.

5.33 Finally, we note that taking such an approach would suggest, incorrectly, that Ofcom is unable to find a CP in breach of a General Condition in any case where it has not previously provided specific guidance. In any event, we consider that the requirement set out in GC3.1(c) is sufficiently clear on its face on how it applies in this context.

Did reliance on [✂Data Centre 3] constitute a potential single point of failure?

5.34 Three has not disputed that avoiding a single point of failure is a key aspect of ensuring resilience. In fact, Three has emphasised that in its view its network is "*[✂] resilient*" and that [✂] resilient networks are "*effective in addressing and mitigating reasonably foreseeable risks."* It also notes that "*[✂] resilience is also the industry standard followed by other mobile network operators ("MNOs") and service providers."*[61]

[59] Three's voluntary submission dated 15 March 2017, paragraph 5. Three also stated that it would be happy to work with Ofcom to develop such guidance and that in the meantime it would be happy to give such undertakings as necessary to maintain sufficient diversity.
[60] *"Changes to General Conditions and Universal Services Conditions"*, Statement dated 25 May 2011, paragraph 5.12.
[61] Introduction to Three's response to the First S135 Notice, 18 January 2017, page 1.

5.35 Three argued that its Emergency Call Service did not, in fact, rely on a single route, location or point of handover for the following reasons:

5.35.1 the [✂] resilience of the [✂APN] meant that *"provided that [✂Data Centre 3] remained available, a break in any single point of Three's [✂APN] would lead to the automatic re-routing of calls including emergency calls";*[62]

5.35.2 prior to the Incident, in the "*unlikely event of a failure of [✂Data Centre 3]* ",[63] Three could have "*re-routed the emergency call traffic and implemented the new routing solution in less than [✂], and likely significantly less*";[64] and

5.35.3 since the Incident, Three has maintained the Interim Solution, meaning that "*…if [✂Data Centre 3] were to fail, [Emergency Call Traffic] would be automatically re-routed to BT via Three's data centres in [✂] and [✂].*"[65]

5.36 Having considered Three's submissions, we consider that Three's Emergency Call Service did in fact rely on a single point of handover at the time of the Incident.

5.37 We acknowledge that the [✂APN] itself was [✂] resilient, and that a single break in the [✂APN] fibre would lead to automatic re-routing of calls, and would therefore not prevent Emergency Call Traffic from reaching [✂Data Centre 3].

5.38 However, it is clear from the information provided by Three during the course of the Investigation that, prior to the Incident, all possible routes for Emergency Call Traffic to reach a BT CHA passed through one single location ([✂Data Centre 3]).[66] The Incident highlighted that Three's Emergency Call Service was dependent on a single set of premises for dealing with Emergency Call Traffic routed via the [✂APN].

5.39 Consequently, a failure to maintain access to Three's Emergency Call Service could have occurred in (at least) the following situations:

5.39.1 if the [✂APN] suffered a simultaneous dual fibre break (as occurred in the Incident); or

5.39.2 if [✂Data Centre 3] were to become unavailable, for example due to loss of power or physical unavailability.

5.40 We note that the EC-RRG Resilience Guidelines specifically reference emergency call traffic and emphasise that CPs should, wherever reasonable, avoid the concentration of essential equipment in a single set of premises,[67] thus recognising the risks this may entail.

5.41 We do not consider that the possibility of Three being able to manually re-route Emergency Call Traffic within [✂] in the event of a failure of Emergency Call Traffic

[62] Three's voluntary submission dated 15 March 2017, paragraph 31.
[63] Three's voluntary submission dated 15 March 2016, paragraph 32.
[64] Three's voluntary submission dated 15 March 2017, paragraph 34.
[65] Three's voluntary submission dated 15 March 2017, paragraph 35.
[66] See Section 4 paragraph 4.11 and Figure A3 in Annex 2.
[67] *"EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure",* March 2008, paragraph 7.1.6(ii). See https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61013/telecoms_ecrrg_resilience_guidelines.pdf.

reaching [✂Data Centre 3] meant that, at the time of the Incident, Three's Emergency Call Service was not reliant on a potential single point of failure.

5.42 The ability to manually implement alternative routing in the event of any failure at [✂Data Centre 3], in however short a period, would not deliver *uninterrupted* access to the emergency organisations. Therefore, should Three's assertion that it can implement an alternative routing within the stated [✂] (or less) of a failure at [✂Data Centre 3] be correct it would nevertheless cause an interruption to service. This, in Ofcom's view, highlights the fact that at the time of any such failure [✂Data Centre 3] would represent a single point of failure and give rise to a lack of diversity in Three's network design.

5.43 We accept that maintaining the Interim Solution has increased the diversity and resilience of Three's Emergency Call Service, but this does not affect our findings about the adequacy of the network design up to and at the time of the Incident.

5.44 In conclusion, we consider that Three's reliance on [✂Data Centre 3] at the time of the Incident constituted a potential single point of failure for its Emergency Call Service. We note that Three's network configuration for Emergency Call Traffic has been in place since [✂before 2011].[68]

The resilience of Three's Emergency Call Service

5.45 Three recognises that EC-RRG Resilience Guidelines state that "*the key is to avoid single points of failure*" but argues that this is *"very general guidance"* and provides "*no further detail as to what precisely is meant by "single point of failure" and/or the extent to which a network may vary the degree of diversity depending on the different levels of risk of failure at different points on the network*".[69]

5.46 In this context, Three has submitted that its reliance on [✂Data Centre 3] "*never placed 'uninterrupted access to the emergency services' at any real risk*" due to the *"inherent resilience"* of its network architecture on the [✂APN], including the "*exceptional resilience"* of [✂Data Centre 3].

5.47 As such, we understand Three's submission to be that, within the context of its network architecture, it would not be 'necessary' within the meaning of GC3.1(c) to require additional diversity (such as an automatic re-routing capability) for its Emergency Call Service to be sufficiently resilient.

5.48 We have therefore considered Three's representations about the likelihood of failure of Three's Emergency Call Service, the actual or potential impact of their occurrence and whether, taking these into account, Three's Emergency Call Service was 'sufficiently resilient' in the context of the resilience measures Three had in place at the time.

[68] See Section 4, paragraph 4.12.
[69] Three's voluntary submission dated 15 March 2017, paragraph 28 and 29.

5.49 First, in relation to the [✂APN], Three has argued that:

5.49.1 the [✂APN] is a '[✂] resilient [✂]', which is "*effective in addressing and mitigating reasonably foreseeable risks and as such are designed to comply with section 105A ... and GC3.1*";[70]

5.49.2 [✂] resilience is the industry standard followed by other mobile network operators ("MNOs") and service providers;[71]

5.49.3 Three's Core Network uses a transmission technology that provides pre-configured [✂automatic re-routing around the APN], e.g. [✂];[72] and

5.49.4 the Incident was "*wholly unique*", caused by an "*unprecedented simultaneous dual fibre break*", and was caused by circumstances outside of Three's control (i.e. the site access restrictions imposed by the third party infrastructure owner in relation to Fibre Break #1).[73]

5.50 Second, in relation to [✂Data Centre 3], Three has submitted that:

5.50.1 [✂Data Centre 3] is a [✂].[74]

5.50.2 If a route carrying Emergency Call Traffic were to fail for any reason (including failure of the "passive" equipment within [✂Data Centre 3]), the network would automatically switch the traffic to one of the pre-configured alternative routes, with no disruption to services.[75]

5.50.3 Due to the resilience of [✂Data Centre 3] and Three's equipment located in [✂Data Centre 3] there was "*no real risk of [✂Data Centre 3] failing to hand-over Three's emergency call traffic to BT*".[76]

5.51 Three has further argued that, in the event of a power failure at [✂Data Centre 3], connectivity would be maintained by the use of [✂], [✂] and [✂]. Moreover, if these should fail, Three submitted that its [✂] would ensure there would be no loss of service.[77] It maintains that the resilience of Three's data centres (including but not specifically relating to [✂Data Centre 3])[78] is:

5.51.1 *"demonstrated by the fact that there has never been a complete loss of power at a data centre owned or shared by Three which has resulted in a loss of emergency voice call connectivity*";[79] and

[70] Introduction to Three's response to the First S135 Notice, 18 January 2017, page 1.
[71] Introduction to Three's response to the First S135 Notice, 18 January 2017, page 1.
[72] Three's response to question 1 of the Second S135 Notice,17 February 2017, pages 2 and 3.
[73] Three response to question 6(a) of First S135 Notice, 18 January 2017.
[74] Three's response to question 1 of the Third S135 Notice, 10 March 2017.
[75] Three's response to question 1b of Ofcom's Third S135 Notice, 10 March 2017.
[76] Three's voluntary submission dated 15 March 2017, paragraph 3. See also Annex 2, paragraph A2.13.
[77] Three's voluntary submission dated 15 March 2017, paragraphs 22 and 23.
[78] See Annex 2, paragraphs A2.21 and A2.22.
[79] Three's voluntary submission dated 15 March 2017, paragraph 24.

5.51.2 *"further demonstrated by the major incidents that they have withstood"*[80] without impact on the conveyance of Emergency Call Traffic.[81]

5.52 Finally, as noted above, Three has submitted that in the "*unlikely event of a failure of [✂Data Centre 3]",* Three could have "*re-routed the emergency call traffic and implemented the new routing solution in less than [✂], and likely significantly less*",[82] meaning there would be no interruption to Emergency Call Traffic.

5.53 We have considered Three's submissions carefully. However, our assessment of whether Three's network configuration was sufficiently resilient has to be made keeping in mind the critical importance to public health and security of access to emergency organisations.[83] Within that context, we have considered whether the possibility of network failure is so remote as to justify the potential single point of failure built into the network architecture Three had in place in relation to its Emergency Call Service.

5.54 We recognise that the Incident represented an unfortunate and unlikely set of circumstances, where:

5.54.1 there were two fibre breaks occurring in quick succession on the [✂APN];[84]

5.54.2 there were unforeseen delays in accessing the site of Fibre Break #1, which were outside of Three's control;[85] and

5.54.3 Three was unfortunate with where the two fibre breaks were located, in that they isolated [✂Data Centre 3] from the rest of the network.[86]

5.55 We also recognise that Three had in place resilience measures in relation to both the [✂APN] and [✂Data Centre 3] and, in particular, that:

5.55.1 using a [✂] diverse fibre network helps underpin the resilience of the network in the event of incidents such as this;[87]

5.55.2 Three is using [✂] technology which is widely used across the industry;

5.55.3 [✂Data Centre 3] has measures in place in terms of diverse connectivity, top-tier power and cooling resilience,[88] fire detection and suppression, and security systems; and

---

[80] Three's voluntary submission dated 15 March 2017, paragraph 25. See also Annex 2, paragraph A2.21.2.
[81] Three's voluntary submission dated 15 March 2017, Annex 2, slide 1.
[82] Three's voluntary submission dated 15 March 2017, paragraph 34.
[83] We note that the emergency call numbers, 999 and 112, are fundamental elements of ensuring access to the emergency services. There is an extremely high level of recognition of the numbers by UK citizens and they can be dialled speedily, compared to the eleven digits typically required for the telephone number of a local police or fire station (which the caller is likely to need to look up).
[84] See Section 4, paragraph 4.13.
[85] See Annex 2, paragraph A2.29.
[86] See Annex 2, paragraph A2.6 and Figure A2.
[87] For example, following Fibre Break #1, Three could convey emergency calls [✂] for onward conveyance to BT via [✂Data Centre 3].
[88] Initially it appeared from the service level agreement (SLA) with [✂Third Party 1] (provided as Annex 2 of Three's response to question 3 of the Second S135 Notice, 15 February 2017) that Three had not purchased [✂]. Notwithstanding the text in the SLA, Three subsequently provided

5.55.4 the presence of alternative handover points to BT on other parts of Three's Core Network means that it would potentially be possible to manually re-configure the routing of Emergency Call Traffic from the [✂APN] to alternative handover points.

5.56 However, in the context of the potentially severe impact of a failure of Three's Emergency Call Service, we do not consider that Three's Emergency Call Service was sufficiently resilient.

5.57 First, despite Three's submissions on the 'inherent resilience' of the [✂APN] and 'exceptional resilience' of [✂Data Centre 3], failures of networks, equipment and premises, even well protected and resilient ones, can and do occur – as the Incident itself demonstrates. We are aware of a number of instances where entire telecommunications buildings have failed or been shut down for a variety of reasons outside of their control, despite being acknowledged themselves as robust and resilient structures.

5.58 Second, we consider that the potential impact of a network failure resulting in an interruption to access to emergency organisations is extremely high. This is because the potential consequences of delay in reaching emergency organisations may be severe for citizens and consumers, resulting in life-threatening situations.[89] We note that even a delay of up to [✂], which Three acknowledged would likely be the case in the event of a complete failure of [✂Data Centre 3], could mean the difference between life and death in extreme scenarios. Even in a less serious scenario, failure to connect with emergency organisations may cause anxiety and emotional distress for consumers.[90] Any such failure of [✂Data Centre 3], which is a core part of Three's network, has the potential to affect a significant number of customers. In that regard we note that [✂Data Centre 3] covers the Emergency Call Traffic for a significant proportion of Three's active customer base ([✂] customers at the time of the Incident, which represented around [✂ a significant proportion] of Three's active customer base).

5.59 As a matter of principle, and in order to maintain, to the greatest extent possible, uninterrupted access to emergency organisations, we consider that the potential severity of a failure of a core part of the network necessarily requires CPs to ensure they avoid, so far as possible, reliance on a potential single point of failure. [91] As set out in paragraph 5.44 above, Three did rely on a potential single point of failure as, up until the date of the Incident, all Emergency Call Traffic (as defined in paragraph 1.6), was routed through [✂Data Centre 3] .

---

confirmation from [✂Third Party 1] showing that this is nevertheless provided to Three at [✂Data Centre 3] (e-mail provided to Ofcom on 30 May 2017). See also Annex 2, footnote 158.

[89] The time taken for emergency organisations to reach incidents can have a significant impact on the outcome. For example, data from the London Fire Brigade shows that nearly two-thirds of deaths and around half of serious injuries arising from fires in dwellings occur when there has been a delay of 10 minutes or more in calling the fire brigade. Fire Facts: incident response times 2005-2013; London Fire Brigade: https://files.datapress.com/london/dataset/incident-response-times-fire-facts/London_Fire_Brigade_Fire_Facts_Incident_response_times_2013.pdf page 4.

[90] See Section 6, paragraph 6.28.2.

[91] Industry guidance issued by EC-RRG also recognises this and states that CPs should: "*…give particular attention to the security of 999/112 emergency and safety of life traffic, for example by using techniques such as priority routing, repeat attempts, alternative routing and trunk reservation, and by avoiding dependence on a single set of premises for dealing with emergency traffic."* See "*EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure",* Guidance March 2008, paragraph 7.1.6 (ii).

5.60 We also note that Three has not argued that it would be impossible to have avoided routing all its Emergency Call Traffic through [✂Data Centre 3]. Rather, Three has argued that it was not 'necessary' to establish alternative routes in order to comply with its obligations in GC3.1, in light of its view of the low risk of failure to connect emergency calls via [✂Data Centre 3], and its claimed ability to manually recover within [✂]. We have considered the proportionality of taking such alternative steps as part of Step 2 below.

5.61 Therefore, whilst we accept that Three considered that its network configuration prior to the Incident represented a low risk of failure and that the circumstances associated with the Incident were unique, we nevertheless do not consider it appropriate for Three to route all its Emergency Call Traffic through a single location, without alternative routing options immediately available, or to rely on being able to institute additional routes within [✂].

Conclusion

5.62 In the light of the above, we have found that:

5.62.1 Three routed all Emergency Call Traffic (as defined in paragraph 1.6) through one single location ([✂Data Centre 3]) thereby leaving the service in the Affected Area vulnerable to a single point of failure in the event that Emergency Call Traffic, for whatever reason, should be unable to be routed via [✂Data Centre 3];

5.62.2 we do not consider it appropriate for Three to route all its Emergency Call Traffic through a single location, without alternative routing options immediately available, or to rely on being able to institute additional routes within [✂]; and

5.62.3 as such, Three did not, at the time of the Incident, have sufficient resilience in the routing for its Emergency Call Traffic.

5.63 Having reached this view, we move to Step 2 to consider whether it was technically feasible for Three to ensure its Emergency Call Service was sufficiently resilient and, if so, whether it was within its reasonable control to do so.

Step 2: Did Three take all necessary steps to ensure sufficient resilience?

5.64 Where we have established that a CP's provision of its emergency call service was not sufficiently resilient, we need to consider whether the CP had taken all necessary steps to maintain, to the greatest extent possible, uninterrupted access to the emergency services. If not, this would place the CP in breach of the requirements in GC3.1(c).

5.65 We will consider that a CP is in breach of GC3.1(c) if it has a single point of failure in its emergency call routing, unless we can be satisfied that it would not have been (a) technically feasible, or (b) within the CP's reasonable control to ensure sufficient resilience.

Would it have been technically feasible for Three to have sufficient resilience in place?

5.66 When examining technical feasibility, our first step is to establish whether it was technically possible for the CP to improve the resilience of its emergency call routing.

For instance, we will consider whether a CP could have added further diversity into its emergency call routing by using alternative routes or putting in place further back-up routes or additional routing to BT interconnect points, or implementing additional risk management actions or processes.

5.67 To the extent we find it was technically possible, our second step is to consider whether it would have been proportionate,[92] in light of the circumstances, to take such steps to improve the resilience of its network.

Was it technically possible for Three to take additional steps to ensure sufficient resilience?

5.68 In this case, it is clear that it was technically possible to establish an alternative transmission route for Three's Emergency Call Traffic to BT CHAs that did not rely on [✂Data Centre 3]. This is apparent from the following:

5.68.1 Three has several pre-existing points on its Core Network through which it routes emergency calls to BT CHAs.[93]

5.68.2 Following the Incident, Three was able to implement an alternative transmission route for its Emergency Call Traffic (the Interim Solution). The Interim Solution established an additional route which can be used to automatically re-route Emergency Call Traffic to pre-existing handover points on Three's core network (e.g. the BT interconnect points in [✂], accessed via Three's sites in [✂] and [✂]), avoiding the [✂APN] and [✂Data Centre 3].[94]

5.68.3 Three informed us that the Interim Solution was operating effectively and that it was maintaining this fix pending the outcome of the Investigation.[95] Three also stated that it would be willing to maintain the Interim Solution (i.e. maintain the automatic re-routing of Emergency Call Traffic) and/or add additional routes manually.[96]

5.69 Although Three has various measures in place to manage risk to network availability,[97] including having *"a dedicated Risk Board to identify, address, mitigate and monitor on an ongoing basis business risks, including risks relating to the conveyance of emergency call traffic",*[98] we note that Three has been unable to provide any evidence that Three's Risk Board was provided with any report, risk assessment or audit which relates specifically to its conveyance of emergency calls (or the network over which emergency calls are carried). For example, Three has informed us that:

[92] In the statement *"Changes to General Conditions and Universal Services Conditions"*, Statement dated 25 May 2011, paragraph 5.19 we stated that "*[t]o ensure proportionality, any assessment of "all necessary measures" will need to take into account the cost and benefits of maintaining availability in the context of the network or services in question".*
[93] Three's response to question 10 of the First S135 Notice, 16 December 2016.
[94] See Annex 2, Figure A5.
[95] Introduction to Three's response to the First S135 Notice,18 January 2017, page 3.
[96] Three's voluntary submission dated 16 March 2017, paragraph 46.
[97] Covering areas such as having identified responsibly for risk management up to senior levels, Incident and Crisis Management and service level agreements with suppliers. See Annex 2 for further details.
[98] Three's response to question 12b of the First S135 Notice, 18 January 2017, page 14.

5.69.1 [✂];[99] and

5.69.2 [✂].[100]

5.70 Consequently, we are concerned that Three has not been able to identify any risk assessment relating to emergency calls (or the network over which emergency calls are conveyed) that has been discussed at the Risk Board. This suggests that:

5.70.1 risks relating to network availability have not been frequently considered at senior levels within Three; and

5.70.2 Three could have done more to assess risk relating to the availability of the network carrying Emergency Call Traffic.

Would it have been proportionate for Three to take additional steps?

5.71 Given that we consider it would have been technically possible for Three to have taken additional steps to ensure sufficient resilience, we move on to consider whether it would have been proportionate for Three to take these steps to ensure sufficient resilience, taking into account factors such as complexity, resourcing and cost. We note in this context that any consideration of proportionality needs to be considered against the objective of GC3.1(c) and the vital public interest that it serves.

5.72 We accept that there may be occasions where certain steps would be disproportionate, such as the deployment of protection paths in the access network to all households. However, in Three's case, it is clear that the lack of resilience identified relates to a part of the network where we would not have expected any risk of single points of failure to arise.[101]

5.73 With regards to its Interim Solution, Three initially argued that it was "*a costly, complex and manually intensive interim fix"* and that its post-incident analysis had confirmed that the fix was unnecessary as "*the existing systems are sufficient absent an exceptionally unlikely event such as that which took place in this case."*[102]

5.74 However, we note that:

5.74.1 Three has not quantified the costs involved in managing or maintaining the Interim Solution;

[99] Three's response to question 5a and 5c of the Second S135 Notice, 20 February 2017.
[100] Three's response to question 4 of the Second 135 Notice, 20 February 2017.
[101] Within a CP's core network, our starting point is that there should be diversity in the routing of emergency call traffic wherever possible (e.g. that the network used for emergency call traffic does not rely on a single route, a single point of handover or on routing all such calls or associated signalling traffic through a single location thereby leaving the service vulnerable to a single point of failure). This is because: (i) a very large number of customers will be exposed to the single point of failure; (ii) the design and architecture of the technology used will typically support high levels of diversity; and (iii) while it will not be cost free, the amount of additional physical infrastructure needed to avoid single points of failure is likely to be limited. Together these factors mean the cost per customer of avoiding a single point of failure will be relatively low.
[102] Introduction to Three's response to the First S135 Notice, 18 January 2017, page 3.

5.74.2 whilst Three provided us with a preliminary post-incident analysis of actions undertaken, it informed us that it does not have any further written report following the Incident setting out this conclusion;

5.74.3 the Interim Solution was introduced in an emergency situation, when it was operating under intense time pressure. If Three was to introduce such a solution in a pre-planned manner, we consider it is likely to incur lower costs as it would give Three a greater opportunity to seek out the optimum solution for the circumstances, and do so using its usual planning processes;

5.74.4 it took around [✂] for Three to implement the Interim Solution following the Incident;[103]

5.74.5 in later submissions, Three submitted that, in the event of a failure of [✂Data Centre 3], Emergency Call Traffic could be re-routed manually, following a 'root cause analysis' and a 'fix process'. Three has submitted that the root cause analysis would have taken 'only [✂]' and the fix process (the manual re-routing) would be implemented in less than [✂];[104]

5.74.6 Three has stated that it would be happy to give such undertakings as we consider necessary to maintain sufficient diversity in its network architecture, including maintaining the automatic re-routing of Emergency Call Traffic.[105]

5.75 Whilst we recognise that Three would have incurred some costs in setting up and maintaining an alternative routing option on a permanent basis (whether or not the same or a similar solution to the Interim Solution), the above facts suggest to Ofcom that it would not be unduly expensive or complex for Three to put in alternative routings for its Emergency Call Traffic, particularly when balanced against the critical importance of maintaining access to emergency organisations.[106]

5.76 More broadly, we consider that it would not have been prohibitively expensive for Three to have taken additional steps to further manage risks relating to the availability of the network for Emergency Call Traffic. For example, Three could have ensured, within its pre-existing risk management structures, that there was senior visibility at the Risk Board of risk assessments carried out relating in whole or in part to the availability of the network carrying Emergency Call Traffic.

5.77 On the basis of the evidence available to us and weighing up the likely cost and complexity of adding an alternative route to the network against the potential harm to consumers of a failure in Three's Emergency Call Service, we conclude that it would have been proportionate for Three to take additional steps to ensure sufficient resilience in its Emergency Call Service.

Conclusion on technical feasibility

5.78 In the light of the discussion above, we have found that it would have been technically feasible for Three to have avoided routing its Emergency Call Traffic to BT CHAs through one single location at [✂Data Centre 3]. In addition, we consider that

[103] Estimated timing based on Three's response to question 4 of the First S135 Notice, 18 January 2017.
[104] Three's voluntary submission dated 15 March 2017, paragraphs 32-34.
[105] Three's voluntary submission dated 15 March 2017, paragraph 46.
[106] See paragraph 5.58.

Three could have taken further steps to manage risk to its Emergency Call Service, such as introducing regular senior-level review of risk assessments considering the conveyance of Emergency Call Traffic on Three's network.

Was it within Three's reasonable control to ensure sufficient resilience was in place?

5.79 Where we have established that there was a single point of failure in a CP's emergency call routing in a location where it would have been technically possible and proportionate to have secured further diversity, it follows that the CP did not have sufficient resilience in its emergency call service. Where this is the case we will consider that the CP is in breach of GC3.1(c), unless we can be satisfied that it would not have been within the CP's reasonable control to have secured sufficient resilience.

5.80 In this case we have, in the light of the available evidence, concluded that Three has full operational control of its network and equipment involved in its Emergency Call Service and that there are no external influences or contractual barriers to taking action to improve the resilience of its network. In particular, we note that:

5.80.1 Three's Core Network is run and maintained by Three;[107]

5.80.2 Three purchases [✂] which it uses for transmission of its Emergency Call Traffic from several providers. Whilst those providers are responsible for the maintenance and servicing of this fibre, Three retains control over the configuration of routing for its Emergency Call Traffic;

5.80.3 alternative physical paths to BT CHAs already existed in Three's Core Network (i.e. it would not need to purchase new fibre, establish new points of presence, etc.);

5.80.4 Three has suggested that it would be happy to maintain the Interim Solution; and

5.80.5 Three has informed us that it would be able to manually configure additional routes for Emergency Call Traffic within [✂].

5.81 We recognise that in the event of actual fibre breaks, such as those which occurred during the Incident, the repair of these breaks on the [✂APN] is subject to service level agreements between its service provider and Three. We also recognise that, with regards to Fibre Break #1, the service provider was reliant on gaining access to third party infrastructure to repair the fibre. However, while this could, in certain circumstances, affect Three's ability to restore service quickly, it does not have any impact on Three's ability to plan its network or introduce alternative routes for Emergency Call Traffic as outlined in paragraph 5.68 above.

5.82 In the light of the above, we consider that it was within Three's reasonable control to ensure sufficient resilience was in place for its Emergency Call Service.

Conclusions on a breach of GC3.1(c)

5.83 Taking all the above considerations into account, we conclude that Three failed to take all necessary measures to maintain, to the greatest extent possible,

[107] Annex 1 of Three's response to question 5 of the First S135 Notice,18 January 2017.

uninterrupted access to emergency organisations. This is based on the following considerations:

5.83.1 Three failed to ensure sufficient resilience in its network as it was routing all Emergency Call Traffic (as defined in paragraph 1.6 above) through one single location ([✂Data Centre 3]), thereby leaving the service vulnerable to a single point of failure;

5.83.2 there were no alternative routes pre-configured on Three's network which, in the event [✂Data Centre 3] was unavailable, would allow Emergency Call Traffic to be automatically re-routed to BT interconnect points without interruption to service; and

5.83.3 it would have been technically feasible and within Three's reasonable control to have ensured sufficient resilience in the provision of its Emergency Call Service.

5.84 Given this, we have concluded that Three contravened GC3.1(c) from 26 May 2011 until Three introduced an additional routing option for Emergency Call Traffic on 6 October 2016.

Section 6

Penalty

Summary

6.1 Ofcom's decision is that we should impose a penalty of £1.89 million on Three for its contravention of GC 3.1(c). The calculation of this figure includes a 30% discount to reflect Three accepting liability and entering into a voluntary settlement with Ofcom.

6.2 Our decision aims to incentivise CPs to comply with their regulatory obligations and is guided by the principal duty of furthering the interest of citizens and consumers. When setting a penalty that would achieve that objective, we have considered a number of factors in the round.

6.3 In particular, we consider that a contravention of GC3.1(c) is a serious matter, given the potential for significant harm. In this case, Ofcom has concluded that Three failed to ensure sufficient resilience in its emergency call routing during the Period of Infringement, which is a long and sustained period, and that this failure was in breach of GC3.1(c).

6.4 Although Three had taken steps to build resilience into its network, the Incident itself highlighted that Three's Emergency Call Service was dependent on a single set of premises for dealing with Emergency Call Traffic (as defined in paragraph 1.6 above). It is clear from the information provided by Three during the course of the Investigation that, prior to the Incident, all possible routes for Emergency Call Traffic to reach a BT CHA passed through [✂Data Centre 3].

6.5 Additionally, Three has not been able to identify any risk assessments relating to emergency calls (or the network over which emergency calls are conveyed) that has been discussed at its Risk Board. This suggests that Three could have taken further steps to review risks relating to the resilience of its network for its Emergency Call Service during the Period of Infringement.

6.6 In mitigation, we have taken into account that Three appears to take the requirement to ensure availability of its Emergency Call Service seriously, and that the breach identified does not appear to have been deliberate or reckless. Three has also cooperated fully with us throughout the investigation.

6.7 Our assessment also takes account of the fact that Three has proposed to keep the Interim Solution in place and/or add additional pre-configured routes which will automatically protect against a failure of [✂Data Centre 3].

6.8 Our view is that the conduct warrants the imposition of a penalty:

6.8.1 to reflect the seriousness and duration of the infringement;

6.8.2 to reflect the potential harm caused by the contravention;

6.8.3 which takes into account that Three is a large CP that services millions of customers, with an annual turnover in excess of £2 billion;[108] and

[108] See paragraph 6.46.

6.8.4 which is sufficiently substantial to incentivise compliance with regulatory obligations by Three and other CPs in future; but

6.8.5 which reflects our view that the contravention did not occur deliberately or recklessly; and

6.8.6 acknowledges Three's cooperation throughout the Investigation.

6.9 Accordingly, and as set out more fully below, we are imposing a penalty of £1.89 million on Three. Our view is that this would be appropriate and proportionate to the contravention in respect of which it is imposed, and will incentivise both Three, and the wider industry, to ensure they are complying with GC3.1(c) on an ongoing basis.

Consideration of whether to impose a penalty

6.10 GC3.1(c) imposes strict standards on CPs. As such we expect a CP to be able to demonstrate that it has done everything it possibly can to ensure that their customers have uninterrupted access to emergency organisations via the 999 and 112 numbers. As set out in Section 5 above, telephone access to emergency organisations is of critical importance to public health and security and any period where customers are unable to access emergency organisations could potentially have catastrophic consequences for individuals.

6.11 Any contravention of GC3.1(c) is therefore potentially serious. The level of seriousness is likely to increase wherever a significant number of customers are affected, the CP has been in contravention over a longer period of time and/or the contravention was deliberate or reckless.

6.12 In this case, although Three does not appear to have acted deliberately or recklessly, the Incident exposed a weakness in its routing for Emergency Call Traffic, which had the potential to affect around [✂a significant proportion] of its active customer base, and remained ongoing during the period from 26 May 2011 to 6 October 2016.

6.13 Three has submitted that it would be unfair to impose any penalty in this case as Ofcom has not issued guidance on the meaning of 'all necessary measures' within GC3.1(c), and that Three was *"at all times complying with the relevant industry standards in the absence of specific guidance from Ofcom"*.[109] It further submits that we should *"contemplate enforcement proceedings such as these only after such guidance is in force."*[110]

6.14 As noted at paragraph 5.13 above, we clearly stated in 2011 that we did not intend to issue guidance on the specific meaning of 'all necessary measures', and that we considered that it is the responsibility of CPs to whom GC3 applies to consider on the facts and circumstances of each case whether they are complying with the obligations imposed therein. Moreover, we do not consider that developing such guidance would be a satisfactory alternative to individual enforcement cases which look in detail at the facts of each individual case.[111] Finally, we note that taking such

[109] Three's voluntary submission dated 15 March 2017, paragraph 4.
[110] Three's voluntary submission dated 15 March 2017, paragraph 5. Three also stated that it would be happy to work with Ofcom to develop such guidance and that in the meantime it would be happy to give such undertakings as necessary to maintain sufficient diversity.
[111] As we set out in our 2011 Statement it is the responsibility of CPs to whom GC3 applies to consider on the facts and the circumstances of each case whether they are complying with its obligations. See "*Changes to General Conditions and Universal Services Conditions"*, Statement dated 25 May 2011, paragraph 5.12.

an approach would, incorrectly, suggest that Ofcom is unable to find a CP in breach of a General Condition, or impose a penalty for that breach, in any case where it has not previously provided specific guidance. In any event, we consider that the requirement set out in GC3.1(c) is sufficiently clear on its face on how it applies in this context.

6.15 In the light of the individual circumstances of this case, we consider that a financial penalty is appropriate and a proportionate response to the nature and seriousness of Three's contravention. It would also help to secure Ofcom's principal duty of furthering the interests of citizens and consumers by incentivising CPs to comply with their regulatory obligations.

Level of penalty

6.16 Having decided that Ofcom should impose a penalty, the next consideration is its amount. In that regard, we have considered the relevant statutory obligations and our Penalty Guidelines.

Statutory provisions

6.17 Section 96A of the Act provides for Ofcom to issue a notification where we have reasonable grounds to believe a person has contravened any of the General Conditions of Entitlement set under section 45 of the Act. Amongst other things, that notification can specify any penalty that Ofcom is minded to impose in accordance with section 96B[112] and must specify a period within which the person notified may make representations in response.

6.18 Section 96C provides for Ofcom to issue a confirmation decision, once the period for making representations has expired, if after considering any representations we are satisfied the person has contravened the relevant condition. A confirmation decision may, amongst other things, confirm imposition of the penalty specified in the section 96A notification or a lesser penalty.

6.19 Section 96A to 96C of the Act apply in relation to any contravention that occurred on or after 26 May 2011 (the date on which those sections came into force) and, in relation to a continuing contravention, the period of contravention from that date.

6.20 Section 97 of the Act provides that a penalty may be such amount not exceeding ten per cent of the notified person's turnover for relevant business for the relevant period as Ofcom determine to be appropriate and proportionate to the contravention for which it is imposed.

6.21 Section 392 of the Act requires Ofcom to prepare and publish guidelines for determining penalties under sections 96A to 96C of the Act. Section 392(6) of the Act requires us to have regard to those guidelines when determining such penalties. The current version of the Penalty Guidelines was published on 3 December 2015.[113]

[112] Section 96A(2)(e) of the Act.
[113] *"Ofcom Penalty Guidelines. S.392 Communications Act 2003"*, Guidelines, 3 December 2015. Available at http://www.ofcom.org.uk/content/about/policies-guidelines/penality/Penalty_guidelines_2015.pdf.

The Penalty Guidelines and relevant factors

6.22 As set out in our Penalty Guidelines, Ofcom will consider all the circumstances of the case in the round in order to determine the appropriate and proportionate amount of any penalty.[114] The particular factors we have considered in this case are:

a) our duties under section 3(3) of the Act: to have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed; and

b) the central objective of imposing a penalty which, as stated in the Penalty Guidelines, is to deter behaviour which contravenes the regulatory requirements and incentivise companies to comply with their regulatory obligations. The amount of any penalty must be sufficient to ensure that it will act as an effective incentive for compliance, having regard to the seriousness of Three's contraventions and its size and turnover;

c) the following, which appear to us to be relevant in determining an appropriate penalty that is proportionate to the contravention in respect of which it is being imposed:

i) the seriousness and duration of Three's contravention;

ii) the degree of harm, whether actual or potential, caused by the contravention;

iii) the extent to which the contravention occurred deliberately or recklessly, including the extent to which senior management knew, or ought to have known, it was occurring or would occur;

iv) whether the contravention continued, or timely and effective steps were taken to end it, once Three became aware of it;

v) whether Three has a history of similar contraventions;

vi) the extent to which Three has cooperated with our investigation; and

vii) the extent to which the level of penalty is appropriate and proportionate, taking into account Three's size and turnover.

Seriousness and duration

6.23 GC3.1(c) is one of the most important regulatory obligations to which a CP offering public telephony services is subject. Uninterrupted access to emergency organisations is a fundamental element of telephony services for UK citizens and serves a vital public interest in the protection of public health and security.

6.24 Accordingly, Ofcom is likely to regard any contravention of GC3.1(c) as inherently serious, because it carries a significant risk of substantial harm to citizens and consumers.

[114] *"Ofcom Penalty Guidelines. S.392 Communications Act 2003"*, Guidelines, 3 December 2015, paragraph 11.

6.25 We have found that, from 26 May 2011 to 6 October 2016, Three did not have all necessary measures in place to ensure uninterrupted access to emergency organisations, in contravention of its obligations in GC3.1(c).[115] This is a prolonged and sustained period, and we have taken this into account when considering the level of the penalty.

6.26 During this period, Three's Emergency Call Service was vulnerable and at unnecessary risk of a service failure due to the fact that all Emergency Call Traffic (as defined in paragraph 1.6 above) was routed to BT interconnect points through one single location (i.e. [✂Data Centre 3]).

The degree of harm, whether actual or potential, caused by the contravention

6.27 The potential consequences of delay in reaching emergency organisations may be severe for citizens and consumers, resulting in life-threatening situations.[116] Therefore, any vulnerability to a single point of failure such as that identified in the Investigation has the potential to give rise to significant consumer harm. The identified vulnerability was in place for over five years and at a location which covers the emergency call traffic for a significant proportion of Three's active customer base ([✂] customers at the time of the Incident, which represented around [✂a significant proportion] of Three's active customer base).

6.28 Consequently, any incident resulting in [✂Data Centre 3], for whatever reason, becoming unavailable, would have the potential to cause significant harm to Three's customers. In particular:

6.28.1 any delay in contacting emergency organisations could cause significant harm to individuals who would, for a period of time, be unable to connect with emergency organisations using 999 and 112 numbers; and

6.28.2 even in circumstances where any delay in contacting emergency organisations does not contribute to any actual physical harm suffered by an individual, we consider it highly likely that an inability to reach emergency organisations by calling 999 or 112 in the event of an emergency would cause emotional distress.[117]

Steps taken by Three to avoid the contravention and the extent to which it occurred deliberately or recklessly

6.29 There is no evidence that Three deliberately or recklessly contravened its obligations under GC3.1(c). Indeed, Three has been clear that it "*recognises the vital importance of maintaining uninterrupted access to emergency call traffic on its network*".[118]

[115] See Section 5, paragraph 5.84.
[116] See Section 5, paragraph 5.58 and footnote 89.
[117] The evidence provided by Three in relation to the Incident supports this view. In particular, it suggests that a number of customers repeatedly attempted calls while the Emergency Call Service was unavailable, which is consistent with increasing anxiety on the part of callers.
[118] Three's voluntary submission dated 15 March 2017, paragraph 2.

6.30 Three has submitted that it had the following systems and processes in place:

6.30.1 a [✂] resilient network in line with industry standards followed by other MNOs and service providers;[119]

6.30.2 an incident management[120] and crisis management procedure[121] in order to restore service quickly;[122]

6.30.3 real-time network alarm monitoring tools and systems;[123]

6.30.4 a hierarchy of protection routes[124] in the event a primary route for emergency calls were to fail;[125]

6.30.5 resilience measures relating to multiple power sources[126] and diverse entry points for fibre cables at [✂Data Centre 3];[127] and

6.30.6 specific service level agreements with third parties covering issues such as availability and incident recovery times.[128]

6.31 Although it considered it unnecessary, Three initially stated that it would maintain its Interim Solution pending the outcome of the Investigation[129] and subsequently stated that it would be happy to give such undertakings as we consider necessary to maintain sufficient diversity in its network architecture, including maintaining the automatic re-routing of Emergency Call Traffic.[130]

6.32 We acknowledge that the points above suggest that Three does take the requirement to ensure availability of its Emergency Call Service seriously,[131] and that the breach identified did not occur deliberately or recklessly. We also acknowledge that Three had taken steps to build resilience into its network. However, it had apparently taken the view that the complete reliance on [✂Data Centre 3] for routing of Emergency

[119] Introduction to Three's response to the First S135 Notice, 18 January 2017. See also paragraph 5.49.2.
[120] Three's response to question 5 of the First S135 Notice, 18 January 2017.
[121] Three's response to question 6c of the Second S135 Notice, 20 February 2017.
[122] See Annex 2, paragraph A2.34.
[123] Three's response to question 13 of the First S135 Notice, 18 January 2017. See also Annex 2, paragraph A2.23.3.
[124] Although as described above in paragraph 4.11 all these are routed through [✂ Data Centre 3].
[125] Three's response to question 2 of the Third S135 Notice, 15 March 2017. See also Annex 2, paragraph A2.12.
[126] Initially it appeared from the SLA with [✂Third Party 1] (provided as Annex 2 of Three's response to question 3 of the Second S135 Notice, 15 February 2017) that Three had not purchased [✂]. Notwithstanding the text in the SLA, Three subsequently provided confirmation from [✂Third Party 1] showing that this is nevertheless provided to Three at [✂Data Centre 3] (e-mail provided to Ofcom on 30 May 2017). See also Annex 2, footnote 158.
[127] Three's response to question 1d of the Second S135 Notice, 17 February 2017. See also Annex 2, paragraphs A2.14 and A2.15.
[128] Three's response to questions 3 and 7 of the Second S135 Notice, 15 February 2017. See also Annex 2, paragraphs A2.23.1 to A2.23.3.
[129] Introduction to Three's response dated 18 January 2017 to the First S135 Notice, page 3.
[130] Three's voluntary submission dated 15 March 2017, paragraph 46.
[131] This is also reflected by the speed by the actions taken by Three to resolve the Incident itself (see Annex 2, paragraphs A2.28 to A2.40).

Call Traffic was not a material risk.[132] We consider this to be Three's main failing in this case.

6.33 In the light of the critical importance of access to emergency organisations to public health and safety and the particularly high standards imposed by GC3.1(c), we consider that the contravention was avoidable and that it would have been technically feasible and within Three's control to put in place additional measures to ensure uninterrupted access to emergency organisations.[133]

6.34 We would expect CPs to take steps to regularly assess their networks, to identify any areas of potential risk and take appropriate action to mitigate such risks, both when this routing was being set up and on an ongoing basis. This is especially the case in relation to emergency calls.

6.35 In that regard, we note Three's submission that it has *"a dedicated Risk Board to identify, address, mitigate and monitor on an ongoing basis business risks, including risks relating to the conveyance of emergency call traffic".*[134] We also note the various measures Three says it has in place to manage risk to network availability. However, we have not seen any evidence to show that Three's Risk Board was provided with any risk assessments or reports specifically relating to its conveyance of emergency calls (or the network over which emergency calls are carried), either at the time GC3.1(c) was expanded to cover mobile operators in 2011, or subsequently.[135]

Steps taken by Three to end the contravention

6.36 In order to resolve the Incident and restore its Emergency Call Service, Three implemented the Interim Solution, routing Emergency Call Traffic to pre-existing handover points on Three's core network.[136]

6.37 This also addressed the specific concern identified as part of the Investigation arising from the potential single point of failure at [✂Data Centre 3].

6.38 Three voluntarily maintained the Interim Solution pending resolution of the Investigation[137] and indicated that it would be willing to give *"such undertakings as Ofcom believes are necessary to maintain sufficient diversity in network architecture."*[138]

History of contraventions

6.39 Ofcom has not previously issued a Confirmation Decision to Three under section 96C of the Act for a contravention of GC3.1(c).

Co-operation throughout the Investigation

6.40 The Investigation was triggered by Three's notification to us of the Incident, in accordance with its obligations under section 105B of the Act. Since the Incident,

[132] Although we note that Three has not provided evidence that this risk was specifically considered in any of its risk management processes.
[133] See Section 5, paragraph 5.83.
[134] Three's response to question 12b of the First S135 Notice, 18 January 2017, page 14.
[135] See Section 5, paragraph 5.69.
[136] See Section 4, paragraph 4.17.
[137] See Section 5, paragraph 5.68.3.
[138] Three's voluntary submission dated 15 March 2017, paragraph 46.

Three has provided us with information in a timely manner and has co-operated fully with the Investigation, including offering to maintain the Interim Solution going forward.

Incentivising compliance

6.41 As we explain in our Penalty Guidelines:

> *"The central objective to imposing a penalty is deterrence. The amount of any penalty must be sufficient to ensure that it will act as an effective incentive to compliance, having regard to the seriousness of the infringement. Ofcom will have regard to the size and turnover of the regulated body when considering the deterrent effect of any penalty."*[139]

6.42 In this respect, as noted above, it appears to us that the breach was not deliberate or reckless and that Three considered its network was sufficiently resilient to maintain uninterrupted access to emergency organisations. We further consider that it is likely that the costs of compliance that were avoided over the period of the contravention would not have been significant.

6.43 However, we do consider that Three failed to ensure that its emergency call routing was sufficiently resilient and, for the reasons set out above, we consider this to be a serious contravention of a regulatory obligation that is critical to public health and security. We therefore consider we should impose a penalty that takes account of the fact this appears not to have been a deliberate breach, but that is also at a level that will incentivise Three, and the wider industry, to ensure that they comply with the requirements of GC3.1(c) at present, and on an ongoing basis.

6.44 We also note that Three's size and relevant turnover is an important consideration in assessing the level of the penalty.

6.45 Ofcom generally regards a regulated body's 'relevant business' to comprise that body's total turnover (that is, across all areas where it is active) as the appropriate reference point for assessing the penalty amount, rather than considering the particular part of the business that is responsible for the infringement.[140] This helps ensure that the level of the penalty has the desired impact of promoting compliance with regulatory requirements within the relevant regulated body and other providers in the sector.

6.46 The Act defines 'relevant period' as the period of one year ending 31 March prior to the date of notification of contravention. However, Three's latest available financial accounts are for the financial year ended 31 December 2015, which state that its total turnover for that period was £2,153 million.[141] For the purposes of determining an appropriate and proportionate penalty in this case, Ofcom considers this figure to constitute Three's relevant turnover. Given this, the maximum penalty we may impose is approximately £215 million.

---

[139] Penalty Guidelines, paragraph 11.
[140] *"Revising the penalty guidelines"* Statement, 3 December 2015, paragraph 2.30. see https://www.ofcom.org.uk/__data/assets/pdf_file/0029/79823/penalty_guidelines_-_statement.pdf
[141] Accounts filed at Companies House. See https://beta.companieshouse.gov.uk/company/03885486/filing-history

Ofcom's conclusions on the level of penalty

6.47 Considering all the above factors in the round, the amount of the penalty we have decided to impose on Three is £1.89 million.

6.48 The calculation of this figure includes a 30% discount to reflect Three accepting liability and entering into a voluntary settlement with Ofcom.

6.49 Ofcom considers that this level of penalty is appropriate and proportionate to the contravention in respect of which it is imposed. Ofcom's objectives in setting it are:

- to impose an appropriate and proportionate sanction that reflects the nature of Three's contravention of GC3.1; and
- to incentivise Three and other CPs to ensure they are complying with their regulatory obligations, particularly GC3.1, at present and on an ongoing basis.

6.50 Ofcom considers that a penalty of this amount will secure these objectives in a proportionate way. It reflects each of the factors described in more detail above. Taking particular account of the seriousness of the contravention and the desire to incentivise compliance, on the one hand, and Three's cooperation and the fact that Three did not act deliberately or recklessly on the other, we consider that a decision to impose a penalty at this level would not be disproportionate. It does not exceed the maximum penalty that Ofcom may impose.[142]

Conclusions

6.51 On the basis of the evidence and reasoning contained in this Explanatory Statement, Ofcom has issued the Confirmation Decision set out in Annex 1. The Confirmation Decision sets out the penalty we have imposed and the steps that should be taken by Three to ensure compliance with GC3.1(c).

[142] Based on Three's turnover in the year ending 31 December 2015 the maximum penalty Ofcom could impose is approximately £215 million.

Section 7

Conclusions and action required by Three

Contravention of GC3.1

7.1 On the basis of the evidence and reasoning contained in this Explanatory Statement, Ofcom determines that during the Period of Infringement, Three has contravened GC3.1(c). It has done so to the extent set out in this document.

Steps that should be taken by Three

7.2 As part of ensuring it takes all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations, Three is required to take the following steps, to the extent it has not already taken them:

a) to ensure that the routing of its Emergency Call Traffic is sufficiently resilient as set out in this explanatory document; in particular, in order to avoid single points of failure, such as that occurring at [✂Data Centre 3];

b) to put in place processes for ongoing review and management of the risks associated with the conveyance of its Emergency Call Traffic, including clear lines of individual accountability up to and including Board or company director level.

7.3 Within one month of the Confirmation Decision (attached at Annex 1), Three is required to provide Ofcom with a description of how the ongoing review and management of the risks associated with the conveyance of its Emergency Call Traffic is to be conducted.

Penalty

7.4 For the reasons set out in this document, Ofcom has imposed a penalty of £1.89 million on Three in respect of its contravention of GC3.1(c).

List of Annexes

Annex 1	Confirmation Decision under Section 96C of the Communications Act 2003 relating to a contravention of General Condition 3.1(c).
Annex 2	Not included in non-confidential version.
Annex 3a	Not included in non-confidential version.
Annex 3b	Not included in non-confidential version.
Annex 4	Not included in non-confidential version.
Annex 5	Not included in non-confidential version.
Annex 5a	Not included in non-confidential version.
Annex 5b	Not included in non-confidential version.
Annex 6	Not included in non-confidential version.
Annex 6a	Not included in non-confidential version.
Annex 6b	Not included in non-confidential version.
Annex 6c	Not included in non-confidential version.
Annex 6d	Not included in non-confidential version.
Annex 6e	Not included in non-confidential version.
Annex 7	Not included in non-confidential version.
Annex 7a	Not included in non-confidential version.
Annex 7b	Not included in non-confidential version.
Annex 7c	Not included in non-confidential version.
Annex 7x	Not included in non-confidential version.

Annex 8	Not included in non-confidential version.
Annex 8a	Not included in non-confidential version.
Annex 9	Not included in non-confidential version.
Annex 9a	Not included in non-confidential version.
Annex 9b	Not included in non-confidential version.
Annex 9c	Not included in non-confidential version.
Annex 9d	Not included in non-confidential version.
Annex 9e	Not included in non-confidential version.
Annex 9f	Not included in non-confidential version.
Annex 10	Not included in non-confidential version.
Annex 11	Not included in non-confidential version.
Annex 11a	Not included in non-confidential version.
Annex 11b	Not included in non-confidential version.
Annex 11c	Not included in non-confidential version.
Annex 12	Not included in non-confidential version.
Annex 12a	Not included in non-confidential version.
Annex 12b	Not included in non-confidential version.

Annex 1

Confirmation Decision under Section 96C of the Communications Act 2003 relating to a contravention of General Condition 3.1(c).

Section 96C of the Communications Act 2003

A1.1 Section 96C of the Communications Act 2003 (the "Act") allows the Office of Communications ("Ofcom") to issue a decision (a "Confirmation Decision") confirming the imposition of requirements on a person where that person has been given a notification under section 96A of the Act, Ofcom has allowed that person an opportunity to make representations about the matters notified, and the period allowed for the making of representations has expired. Ofcom may not give a Confirmation Decision to a person unless, having considered any representations, it is satisfied that the person has, in one or more of the respects notified, been in contravention of a condition specified in the notification under section 96A.

A1.2 A Confirmation Decision:

a) must be given to the person without delay;

b) must include the reasons for the decisions;

c) may require immediate action by the person to comply with the requirements of a kind mentioned in section 96A(2)(d) of the Act,[143] or may specify a period within which the person must comply with those requirements; and

d) may require the person to pay:

i) the penalty specified in the notification issued under section 96A of the Act, or

ii) such lesser penalty as Ofcom consider appropriate in light of the person's representations or steps taken by the person to comply with the condition or remedy the consequences of the contravention, and may specify the period within which the penalty is to be paid.

General Condition 3.1

A1.3 Section 45(1) of the Act gives Ofcom power to set conditions, including General Conditions ("GCs"), which are binding on the person to whom they are applied.

A1.4 On 22 July 2003, shortly before the coming into force of the relevant provisions of the Act, the Director General of Telecommunications (the "Director") published a notification in accordance with section 48(1) of the Act entitled *'Notification setting*

[143] Such requirements include those steps that Ofcom thinks should be taken by the person in order to remedy the consequences of a contravention of a condition.

general conditions under section 45 of the Communications Act 2003'.[144] Under Part II of the Schedule to that notification, the Director set (among others) General Condition 3.1 (GC3.1), which took effect on 25 July 2003.[145]

A1.5 On 29 December 2003, Ofcom took over the responsibilities and assumed the powers of the Director, and notifications made by the Director are to have effect as if made by Ofcom under the relevant provisions of the Act.

A1.6 GC3.1[146] requires that:

> *"The Communications Provider shall take all necessary measures to maintain, to the greatest extent possible:*
>
> *(a) the proper and effective functioning of the Public Communications Network provided by it at all times, and*
>
> *(b) in the event of catastrophic network breakdown or in cases of force majeure the fullest possible availability of the Public Communications Network and Publicly Available Telephone Services provided by it, and*
>
> *(c) uninterrupted access to Emergency Organisations as part of any Publicly Available Telephone Services offered."*

A1.7 Sections 96A to 96C of the Act give Ofcom the powers to take action, including the imposition of penalties, against persons who contravene, or have contravened, a condition set under section 45 of the Act.

Subject of this Confirmation Decision

A1.8 This Confirmation Decision is addressed to Hutchison 3G UK (trading as Three), whose registered company number is 03885486. Hutchison 3G UK's registered office is Star House, 20 Grenfell Road, Maidenhead, Berkshire, SL6 1EH.

Notification given by Ofcom under section 96A

A1.9 On 2 June 2017, Ofcom gave a notification under section 96A of the Act (the "section 96A Notification") to Three as Ofcom had reasonable grounds for believing that Three had contravened GC3.1(c). Specifically, that, between 26 May 2011 and 6 October 2016, Three failed to take all necessary measures to maintain to the greatest extent possible, uninterrupted access to emergency organisations as part of its publicly available telephony service. Ofcom arrived at this provisional conclusion for the following reasons:

A1.9.1 Three failed to ensure sufficient resilience in its network as it was routing all Emergency Call Traffic in the Affected Area through one single location

---

[144] Available at: http://webarchive.nationalarchives.gov.uk/20040104233440/http://www.ofcom.org.uk/static/archive/oftel/publications/eu_directives/2003/cond_final0703.pdf.

[145] A consolidated version of the General Conditions is available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0026/86273/CONSOLIDATED_VERSION_OF_GENERAL_CONDITIONS_AS_AT_28_MAY_2015-1.pdf.

[146] GC3.1 was amended by Ofcom on 26 May 2011 following EU revisions made to article 23 of Directive 2002/22/EC (the Universal Services Directive). GC3.1 has not been subsequently revised.

([✂Data Centre 3]), thereby leaving the service vulnerable to a single point of failure;

A1.9.2 there were no alternative routes pre-configured on Three's network which, in the event [✂Data Centre 3] was unavailable, would allow Emergency Call Traffic to be automatically re-routed to BT interconnect points without interruption to service; and

A1.9.3 it would have been technically feasible and within Three's reasonable control to have ensured sufficient resilience in the provision of its Emergency Call Service.

A1.10 The section 96A Notification also specified the penalty that Ofcom was minded to impose on Three in respect of the contravention of General Condition 3.1(c).

A1.11 The section 96A Notification allowed Three the opportunity to make representations to Ofcom about the matters set out.

Confirmation Decision

A1.12 The period allowed for making representations has now expired. On 9 June 2017 Three confirmed to Ofcom that it would not make any written or oral representations about the matters notified and accepted liability for the contravention by admitting it contravened GC3.1(c) in the period 26 May 2011 to 6 October 2016.

A1.13 Accordingly, Ofcom is satisfied that Three has, in the respects notified in the section 96A Notification, contravened General Condition 3.1(c). Ofcom has decided to give Three a Confirmation Decision, and to impose a financial penalty, in accordance with section 96C of the Act. The reasons are set out in the Explanatory Statement to which this Confirmation Decision is annexed.

Requirements

A1.14 As part of ensuring that it takes all necessary measures to maintain, to the greatest extent possible, uninterrupted access to the emergency organisations, Three is required to take the following steps, to the extent it has not already taken them:

A1.14.1 to ensure that the routing of its Emergency Call Traffic is sufficiently resilient as set out in the Explanatory Statement to which this Confirmation Decision is annexed; in particular, in order to avoid single points of failure, such as that occurring at [✂Data Centre 3];

A1.14.2 to put in place processes for ongoing review and management of the risks associated with the conveyance of its Emergency Call Traffic, including clear lines of individual accountability up to and including Board or company director level, and that

A1.14.3 Within one month of this Confirmation Decision, to provide Ofcom with a description of how the ongoing review and management of the risks associated with the conveyance of its Emergency Call Traffic is to be conducted.

A1.15 The duty to comply with any requirement imposed by a Confirmation Decision is enforceable in civil proceedings by Ofcom for an injunction, for specific performance or for any other appropriate remedy or relief.[147]

Penalty

A1.16 Ofcom has determined that Three must pay a penalty of £1.89 million in respect of its contravention of General Condition 3.1(c).

A1.17 Three has until 5.00pm on 14 June 2017 to pay Ofcom the penalty. If not paid within the period specified it can be recovered by Ofcom accordingly.[148]

Interpretation

A1.18 Words or expressions used in this Confirmation Decision have the same meaning as in the General Conditions or the Act except as otherwise stated in the Explanatory Statement to which this Confirmation Decision is annexed.

Gaucho Rasmussen

Director of Enforcement and Investigations

as decision maker for Ofcom

16 June 2017

[147] Section 96C(6) Communications Act 2003.
[148] Section 96C(7) Communications Act 2003.

Annex 2 - 12

Not included in non-confidential version