



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

Confirmation Decision served on KCOM Group Plc by
the Office of Communications

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

Issue date:

8 August 2017

Contents

Section		Page
1	Executive Summary	1
2	Regulatory Framework	4
3	The Investigation	8
4	Relevant facts	14
5	Analysis and evidence of contravention	32
6	Penalty	55
7	Conclusions and action required by KCOM	65
Annex		Page
1	Confirmation Decision under section 96C of the Communications Act 2003 relating to a contravention of General Condition 3.1(c).	68

Section 1

Executive Summary

- 1.1 This document (the Explanatory Statement) explains Ofcom's decision to issue KCOM Group PLC (KCOM) with a confirmation decision (the Confirmation Decision) under section 96C of the Communications Act 2003 (the Act) because it has reasonable grounds to believe that KCOM has contravened General Condition 3.1(c) (GC3.1(c)) of the General Conditions of entitlement.¹ 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 the emergency organisations as part of any publicly available telephone service that they offer.
- 1.3 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, Ofcom would expect 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.
- 1.4 On 28 December 2015, in line with its obligations under section 105B of the Act,² KCOM notified Ofcom of an incident that led to a loss of access to KCOM's emergency call service on 999 and 112 for its customers in the Hull area on the night of 27/28 December 2015 (the Incident). KCOM provided further updates on 29 December 2015 and a supplementary impact report (the Report) on 25 January 2016.³
- 1.5 In the Report, KCOM explained that its emergency call service for the Hull area failed from 21:58 on 27 December 2015 until 01:43 on 28 December 2015. It attributed this failure to flooding at BT's York Stonebow exchange in the wake of Storm Eva, which hit the UK on 23 December 2015.
- 1.6 Ofcom opened an investigation on 11 February 2016 into whether there was or had been a contravention of KCOM's obligations under GC3.1 and/or section 105A(1)-(3) of the Act (the Investigation).⁴
- 1.7 Based on the evidence received during the Investigation, including the Report and the information from KCOM, British Telecommunications plc (BT) and BT Managed Services Limited (BT MSL), Ofcom considered that there were reasonable grounds for believing that KCOM had contravened GC3.1(c) in the period 26 May 2011 to 28 December 2015 (the Period of Infringement) by failing to take the appropriate measures to maintain uninterrupted access to the emergency organisations on 999

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. 1.pdf

² See paragraphs 2.5 and 2.10 below.

³ A copy of the Report is available at Annex 4.

⁴ 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.

and 112. Accordingly, on 2 June 2017, we issued KCOM with a notification under section 96A of the Act (the 96A Notification)

- 1.8 The 96A Notification set out Ofcom's provisional finding that KCOM failed to meet the high standard imposed on CPs in GC3.1(c) to take all necessary measures to maintain uninterrupted telephone access to the emergency organisations as:
 - 1.8.1 KCOM did not have diverse and resilient routing in place for its emergency call traffic during the period from 26 May 2011 until 28 December 2015 as its call routing included a single point of failure at the BT York Stonebow exchange;
 - 1.8.2 it was technically feasible and within KCOM's reasonable control to have diverse and resilient routing in place for its emergency call traffic during that period which would have avoided the single point of failure; and
 - 1.8.3 KCOM failed to take sufficient steps to enable it to ensure that it had diverse and resilient routing in place for its emergency call traffic.
- 1.9 The 96A Notification set out the steps that Ofcom provisionally concluded KCOM should take to comply with the requirements of GC3.1(c) and Ofcom's provisional view that that is was minded to impose a penalty for the contravention and the amount of that penalty that Ofcom provisionally considered would be appropriate and proportionate. KCOM was given the opportunity to make written and/or oral representations on the notified matters.
- 1.10 KCOM provided written representations on the notified matters on 30 June 2017 (KCOM's Response to the 96A Notification), providing additional information about steps that it said it had taken prior to the Incident to enable it to ensure that it had diverse and resilient emergency call routing in place for its emergency call traffic.
- 1.11 Ofcom has considered KCOM's Response to the 96A Notification but remains of the view that KCOM failed to take sufficient steps to enable it to ensure it had diverse and resilient routing in place for its emergency call traffic and therefore it failed to meet the particularly high standard imposed by GC3.1(c) to take all necessary measures to maintain uninterrupted access to the emergency organisations.
- 1.12 Ofcom is therefore satisfied that KCOM contravened GC3.1(c) during the Period of Infringement. In light of our findings in relation to GC3.1(c), we do not consider it necessary to also consider whether KCOM has contravened section 105A of the Act.
- 1.13 As part of ensuring that it takes all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations, KCOM is required to take the following steps, to the extent it has not already taken them:
 - i) to ensure that the routing of its emergency call traffic is sufficiently resilient (as described in this document); and
 - ii) to put in place processes for ongoing review and management of the risks associated with the conveyance of its emergency call traffic (including putting in place clear lines of individual accountability up to and including Board or company director level).
- 1.14 We have determined that a penalty of £900,000 is appropriate and proportionate to the contravention in respect of which it is imposed. In taking this view, we have had

regard to all the evidence referred to in Sections 2, 3, 4 and 5 of this document, together with Ofcom's published Penalty Guidelines.⁵ The basis for Ofcom's view as to the amount of the penalty is explained in Section 6.

⁵ Penalty Guidelines, 3 December 2015: http://www.ofcom.org.uk/content/about/policies-guidelines/penalty/Penalty_guidelines_2015.pdf.

Section 2

Regulatory Framework

Introduction

- 2.1 This section sets out the legal framework relevant to our 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.

General Conditions of Entitlement

- 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, 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 our investigation, was introduced in its current form on 23 May 2011⁶ and 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."*⁷

- 2.4 GC3.1 implements Article 23 of the Universal Service Directive 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."*

⁶ *Changes to General Conditions and Universal Service Conditions: implementing the revised EU Framework*, 23 May 2011: <http://stakeholders.ofcom.org.uk/consultations/gc-usc/statement>.

⁷ 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.

Sections 105A to 105D

2.5 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 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 Framework⁸ and took effect from 26 May 2011.⁹

2.6 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.”

2.7 Ofcom has published guidance on the application of section 105A of the Act, initially on 10 May 2011 (the May 2011 Guidance)¹⁰ and then again in August 2014 (the August 2014 Guidance).¹¹ The two sets of guidance do not materially differ in terms of the guidance provided in relation to section 105A. In both sets of guidance, the meaning of “security” in the context of sections 105A to 105D is defined as “protecting confidentiality, integrity and availability”.¹²

2.8 The May 2011 Guidance 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

⁸ See paragraphs 4 and 65 of Schedule 1 to the Electronic Communications and Wireless Telegraphy Regulations 2011. See

http://www.legislation.gov.uk/ukxi/2011/1210/pdfs/ukxi_20111210_en.pdf.

⁹ SI 2011/1210. Paragraph 65 of Schedule 1 to the Regulations introduced sections 105A-105D into the Act. See http://www.legislation.gov.uk/ukxi/2011/1210/pdfs/ukxi_20111210_en.pdf.

¹⁰ 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>.

¹¹ 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>.

¹² May 2011 Guidance, paragraph 3.4; August 2014 Guidance, paragraph 3.2.

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.”¹³

2.9 The August 2014 Guidance 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”.¹⁴

2.10 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

2.11 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 May 2011 Guidance and the August 2014 Guidance,¹⁵ the obligations in GC3.1(c) are in this context more onerous than those in section 105A because of the critical nature of emergency services access for end-users.¹⁶ 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.

2.12 Given that this investigation concerns a loss of access to the emergency services for KCOM customers, we have therefore focused our investigation on KCOM's compliance with GC3.1(c) during the period from 26 May 2011¹⁷ until 28 December 2015, i.e. the date that the Incident concluded (“the Relevant Period”). Our analysis in Section 5 below reflects this.

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

¹³ May 2011 Guidance, paragraph 3.15. The requirements of GC3 are discussed below.

¹⁴ 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>.

¹⁵ See paragraphs 2.8 and 2.9 above.

¹⁶ 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”.

¹⁷ As set out in paragraph 2.14 below, Ofcom's powers under sections 96A to 96C of the Act only apply in relation to contraventions that occurred on or after the 26 May 2011.

Ofcom's investigation and enforcement powers

- 2.14 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. These sections do not apply in relation to contraventions which occurred before 26 May 2011.
- 2.15 Section 96A of the Act provides for Ofcom to issue a notification setting out Ofcom's preliminary view of the alleged contravention. The 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.
- 2.16 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.

Section 3

The Investigation

Background

- 3.1 On 28 December 2015, KCOM notified Ofcom under section 105B of the Act of an incident that caused a loss of its emergency call service on emergency call numbers 999 and 112 in the Hull area. KCOM provided Ofcom with further updates relating to the Incident on 29 December 2015 as well as the Report, which was submitted on 25 January 2016.
- 3.2 In the Report, KCOM explained that its emergency call service for the Hull area failed from 21:58 on 27 December 2015 until 01:43 on 28 December 2015. During this period, KCOM end-users were unable to contact emergency organisations using the numbers 999 and 112. KCOM explained that it was only its emergency call service on 999 and 112 that failed and that its ability to support outbound national calls and local Hull calls was not affected during this period.¹⁸
- 3.3 KCOM attributed the Incident to flooding at BT's York Stonebow exchange in the wake of Storm Eva, which hit the UK on 23 December 2015 and led to record levels of flooding in the north of England. The Report stated that:

*"The KCOM emergency call service for the Hull area failed as a result of BT losing their York Stonebow exchange on 27 December due to severe flooding. This telephone exchange is where KCOM hand over their emergency call traffic from the Hull area and where KCOM thought they had purchased resilient services from BT. It is now apparent that BT's York Stonebow exchange was an unknown single point of failure..."*¹⁹

- 3.4 KCOM subsequently provided a Root Cause Analysis report (the RCA) to us on 29 March 2016 that was carried out on its behalf in relation to the Incident.²⁰ The RCA explained that:

*"The root cause is attributed to a single (previously unknown) point of failure within the BT transmission delivery at York Stonebow of the three main emergency interconnect routes for traffic passed into the BT network from KCOM. Whilst traffic was destined to BT exchanges in York, Leeds and Sheffield, this failure physically occurred within the BT York Stonebow Exchange where a nexus existed of 112/999 traffic over voice carrying transmission paths..."*²¹

- 3.5 KCOM reported that the loss of the BT's York Stonebow exchange left 187,406 KCOM lines²² where residential and business customers were unable to make 999

¹⁸ The Report, page 1, Executive Summary and Context.

¹⁹ The Report, page 1, Executive Summary and Context.

²⁰ The RCA is attached to the KCOM First Response, question 8(b). A copy of the RCA can be found at Annex 9.

²¹ The RCA, section 2.

²² KCOM noted in the Report that this number was likely to inflate the effective line count in the Hull area as it includes Private Branch Exchange lines.

calls. It identified a total of 90 calls that were attempted to 999/112 over the period of the Incident.²³

3.6 [redacted]²⁴ [redacted]²⁵

3.7 In the Report, KCOM informed us that, following the Incident, it worked with BT to ensure that it had “*appropriate resilience in place with them at York*” and that it had “*retained resilience using fibres from our national network*”.²⁶ The RCA also explained that “*re-configuration of the transmission routeings identified as root cause, within the BT network has been implemented to ensure a greater degree of physical diversity exists for the three primary routeings to York, Leeds & Sheffield*”.²⁷

The decision to investigate

3.8 Typically, Ofcom receives about 500 reports from CPs under section 105B annually; of these, a minority relate to outages affecting more than 10,000 lines or which last for more than a day.²⁸ Ofcom considers what action to take in respect of each report that it receives, in the light of the incident reported.

3.9 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.

3.10 In this case, KCOM's notification under section 105B of the Act gave Ofcom cause for concern on receipt because of the particular features of the security breach that it had reported. These included:

- the complete loss of its emergency call service on 999 and 112 for the Hull area;
- the number of lines that were affected by the loss;
- the duration of the loss; and
- [redacted]

²³ The Report, paragraphs 19 and 20. 16 of these calls were test calls made by KCOM.

²⁴ [redacted].

²⁵ [redacted].

²⁶ The Report, paragraph 21.

²⁷ The RCA, section 3.5.2.

²⁸ As set out in paragraph 8.3 of the Connected Nations Report 2015 available at: http://stakeholders.ofcom.org.uk/binaries/research/infrastructure/2015/downloads/security_and_resilience.pdf and paragraphs 7.9 and 7.10 of the Infrastructure Report 2014 available at https://www.ofcom.org.uk/data/assets/pdf_file/0011/46010/infrastructure-14.pdf.

- 3.11 Because of the impact on KCOM's services, Ofcom was also concerned about the resilience of KCOM's network. In the Report, KCOM provided a diagram showing KCOM's Hull emergency call network was configured in such a way that all its emergency call traffic passed through the BT York Stonebow exchange. KCOM admitted in its notification that it had not been aware of the single point of failure that led to the loss of the service. Given the apparent lack of route separation for services which are required to provide "uninterrupted access" to the emergency organisations, to the greatest extent possible, Ofcom considered it was appropriate to examine the configuration of KCOM's emergency call network more closely.
- 3.12 In light of the features highlighted above, we decided that it was appropriate to investigate whether KCOM was in breach of its obligations under GC3.1(c) and section 105A.²⁹

Information gathering

- 3.13 As part of our investigation, we used our powers under section 135 of the Act to gather information from KCOM, BT and BT MSL³⁰ to help us assess whether KCOM contravened GC3.1 and/or section 105A of the Act. We set out in Section 4 the factual information provided by KCOM, BT and BT MSL that we rely on in this Confirmation Decision.
- 3.14 We sent KCOM an information request on 11 March 2016 requiring KCOM to provide information relating to how its emergency call traffic was routed through its network, including any points of handover to BT. In addition, we required KCOM to provide:
- A copy of the contract for services held with BT which relates to the conveyance of emergency traffic on BT's network;
 - An organogram showing the teams and/or organs within KCOM with responsibility for the conveyance of emergency call traffic, including the position of each team in the decision-making structure for issues relating to emergency call conveyance;
 - All risk assessments carried out by, or on behalf of, KCOM in relation to the routing and/or conveyance by BT of emergency call traffic for the purposes of deciding whether to contract with BT for these services and all risk assessments, internal and external audits received or carried out by or on behalf of KCOM in relation to the routing and/or conveyance of emergency call traffic since 1 March 2011;
 - Documentation that set out the measures that KCOM had in place to monitor the conveyance of emergency call traffic at the time of the Incident; and
 - Documentation that set out the contingency plans that KCOM had in place at the time of the Incident in relation to network or service failures affecting the emergency call traffic.

²⁹ As set out in Section 2, we have focussed our investigation on GC3.1.

³⁰ KCOM contracted with BT MSL in June 2009 in relation to the operation and management of the KCOM network. See paragraphs 4.40 to 4.52 for further information in relation to this contract.

- 3.15 KCOM responded on 29 March 2016 and a copy of this response (the KCOM First Response) is at Annex 5.
- 3.16 On 21 April 2016, we requested information from BT about the way in which KCOM emergency calls were routed from the KCOM network to BT call handling agents (CHAs).
- 3.17 Specifically, we requested from BT a description of the physical route or routes for conveying KCOM emergency call traffic, as at the date of the information request, from the KCOM network to the BT interconnect sites at York, Leeds and Sheffield.
- 3.18 We also asked whether any changes were made to this physical routing between 25 February 2009 and 27 December 2015, and if so, whether these changes were notified to KCOM or to BT MSL (by virtue of its contractual responsibility for managing the KCOM network).³¹
- 3.19 BT provided a consolidated response to the information request on 20 May 2016.³² A copy of this response (the BT First Response) can be found at Annex 6.
- 3.20 After consideration of the BT First Response, we sent an information request to BT MSL on 15 June 2016, as well as a further information request to BT on 16 June 2016.
- 3.21 We asked BT MSL to provide us with the information that it relied upon in reaching its conclusions in the RCA about the failure of KCOM's emergency call service being attributed to a "...single (previously unknown) point of failure within the BT transmission delivery at York Stonebow...".³³ In particular, we requested the information relied upon, both in the RCA and in any post incident reviews, that related to the routes that were used, or available to be used on the BT network for the conveyance of KCOM emergency call traffic on 27 December 2015 and the transmission paths comprising each such route. Additionally, we asked BT MSL to provide us with any updated version of the RCA and any report supplementary to the RCA that it had produced since 23 March 2016.
- 3.22 We asked BT to provide us with further information about how KCOM emergency call traffic was routed on 27 December 2015. In particular, we requested details of certain transmission paths that were used, or available to be used, for the conveyance of KCOM emergency call traffic on 27 December 2015, and whether these transmission paths had any interdependency with the BT York Stonebow exchange.
- 3.23 BT and BT MSL responded to the further information requests on 23 June 2016. A copy of BT's response (the BT Second Response) can be found at Annex 7 and a copy of the BT MSL response can be found at Annex 8.
- 3.24 On 7 October 2016, we sent KCOM a first Notification under section 96A of the Act (the First Notification) and KCOM sent in written representations on the First Notification on 2 December 2016 (KCOM's First Written Response). A copy of KCOM's First Written Response can be found at Annex 2.

³¹ See paragraphs 4.40 to 4.52 below for details of KCOM's arrangements with BT MSL.

³² BT provided responses to some of the questions on 6 May and 13 May 2016.

³³ The RCA, section 4.3.

- 3.25 After consideration of KCOM's First Written Response we sent BT a further information request on 20 December 2016. We asked BT whether the signalling for the relevant BT transmission paths had remained the same throughout the Relevant Period, incorporating an interdependency on York. We also asked whether there was any protocol in place during the Relevant Period whereby BT notified KCOM (or BT MSL) of maintenance works which could impact BT routes available for KCOM's emergency call traffic. BT provided a partial response on 2 February 2017 as well as a further response on 27 March 2017.³⁴ A copy of BT's 2 February 2017 response, as well as the 6 March 2017 response (both referred to as the BT Third Response) can be found at Annex 3.
- 3.26 On 13 February 2017, we sent both KCOM and BT further formal information requests asking for information to assist with our investigation. We asked both KCOM and BT to provide us with a copy of the *"Technical Master Plan"* currently retained by them which according to the Standard Interconnect Agreement (SIA)³⁵ records the *"physical arrangements and Number Ranges or part thereof, for each of the Traffic Routes on an Interconnect Link..."*³⁶
- 3.27 In addition, we asked KCOM to provide us with:
- 3.27.1 all of documents that were used in producing the report by PA Consulting (the PAC Report) which was annexed to KCOM's First Written Response;
 - 3.27.2 further details as to the *"hand off"* points referred to in paragraph 2.2.2 of the PAC Report;
 - 3.27.3 an explanation as to the purpose of the document entitled Appendix 24D attached to Annex 2 of KCOM's First Written Response.
- 3.28 KCOM responded to the second information request on 20 February 2017 (the KCOM Second Response). A copy can be found at Annex 18.
- 3.29 We asked BT to provide us with an explanation as to what it meant when, in the BT First Response, it said that it had an *"agreement"* in place with KCOM that it could use certain BT routes for the delivery of emergency calls and we requested any written record of this agreement.
- 3.30 BT responded to the fourth information request on 20 February 2017 (the BT Fourth Response). A copy can be found at Annex 19.
- 3.31 This confirmation decision also refers to correspondence between Ofcom and KCOM in 2014 in relation to the measures KCOM has taken to manage cyber security risks³⁷

³⁴ BT also provided a further partial response on 20 January 2017 however this information is consolidated in the two responses we have attached.

³⁵ For further details on the SIA, please see Section 4.

³⁶ Annex A to the SIA, paragraph 5.7.

³⁷ In February 2014, we wrote to CPs to ask about their organisational arrangements for security planning in relation to management accountability and technical capability. KCOM responded in a letter dated 11 March 2014 [3<] (March 2014 Letter). A copy of the March 2014 Letter can be found at Annex 15.

and to material in KCOM's Annual Report 2014/15 on its approach to risk management and the principal risks facing the business.³⁸

Ofcom's provisional conclusions

- 3.32 On 2 June 2017, we sent KCOM a second notification under section 96A of the Act (the 96A Notification).
- 3.33 The 96A Notification set out Ofcom's provisional finding that KCOM failed to meet the obligation imposed on CPs in GC3.1(c) to take all necessary measures to maintain, to the greatest extent possible, uninterrupted telephone access to the emergency services as:
- 3.33.1 KCOM did not have diverse and resilient routing in place for its emergency call traffic during the period from 26 May 2011 until 28 December 2015 as its call routing included a single point of failure at the BT York Stonebow exchange;
 - 3.33.2 it was technically feasible and within KCOM's reasonable control to have diverse and resilient routing in place for its emergency call traffic during that period which would have avoided the single point of failure; and
 - 3.33.3 KCOM failed to take sufficient steps to enable it to ensure that it had diverse and resilient routing in place for its emergency call traffic.
- 3.34 The 96A Notification set out the steps that Ofcom provisionally concluded KCOM should take to comply with the requirements of GC3.1(c). It also set out Ofcom's provisional view that it would be appropriate and proportionate to impose a penalty in respect of the contravention. The 96A Notification gave KCOM the opportunity to make written and/or oral representations on the notified matters.
- 3.35 KCOM provided written representations on the notified matters on 30 June 2017 (KCOM's Response to the 96A Notification). These included additional information about the terms of the Horizon contract³⁹ between KCOM and BT MSL. KCOM submitted that the steps it had taken prior to the Incident to enable it to ensure that it had diverse and resilient emergency call routing in place for its emergency call traffic, included the requirements it had imposed on BT MSL under the terms of the Horizon contract.
- 3.36 In relation to KCOM's First Written Response, KCOM said *"We do not repeat points that Ofcom has already seen or considered, although in some cases we cross-refer to points from KCOM's [First Written Response] that remain relevant."*⁴⁰
- 3.37 This confirmation decision takes account of KCOM's First Written Response and its Response to the 96A Notification. We have summarised and responded to matters raised by KCOM in its representations in Section 5. A copy of KCOM's First Written Response is at Annex 2 and a copy of KCOM's Response to the 96A Notification is at Annex 28.

³⁸ The full KCOM Annual Report for 2014/15 is available at:

<http://www.kcomplc.com/media/1364/kcom-group-plc-annual-report-and-accounts-2014-15.pdf>. We refer specifically to page 35 (see Annex 16) and pages 20 and 21 (see Annex 17).

³⁹ See paragraphs 4.40 to 4.52 for details relating to the Horizon contract

⁴⁰ Paragraph 1.5, KCOM's Response to 96A Notification.

Section 4

Relevant facts

Introduction

- 4.1 This section sets out our understanding of the relevant facts from the evidence we have gathered in our investigation. We set out our assessment of the evidence in Section 5.

Access to the emergency organisations in the UK

- 4.2 In general, when an ordinary telephone call is made between two people, the call will be supported by multiple CPs forming an end-to-end chain of connection. Each individual CP will route the call through its own network, from the point where the call enters the network (the ingress point) to either a corresponding egress point or, if it is the last CP in the chain, connecting with the person being called. The ingress/egress points between CPs' networks are where switches exist that allow calls to be transferred onto the corresponding CP's network. To avoid confusion, we shall use the following terms in this document:
- "Switch Connection(s)"⁴¹: These are designated ingress/egress points where switch equipment exists to allow calls to be switched on to (and off of) a CP's network. Switch Connections will only be available at certain exchanges.
 - "Points of Connection"⁴²: These are points where CPs can hand over their traffic to another CP's network, but where switching equipment does not exist to transfer the call onto the corresponding CP's wider network.
- 4.3 With regards to the routing of emergency calls, similar procedures and practices apply. Historically some CPs provided their own emergency CHA function,⁴³ but today all CPs in the UK purchase CHA services from BT. This means that (where CPs have a network of their own) they need to take their traffic to a BT Switch Connection so that the call can be switched onto the BT network and BT can onward route the call to connect to one of its CHA centres that exist across the UK. BT's CHAs will then answer and forward emergency calls to the appropriate emergency authority.
- 4.4 For Public Switched Telephony Network (PSTN) services, BT only offers Switch Connections at certain specific exchanges around the UK. These specific exchanges will contain the BT switches that allow calls to be switched onto the BT network for onward routing by BT to the relevant CHA. Of particular relevance to this case are

⁴¹ A Switch Connection is defined in the SIA and for the purposes of this Notification we consider that it has the same meaning as a point of interconnect i.e. where calls are switched onto the corresponding network. See paragraph 4.28 below for the definition set out in the SIA.

⁴² Point(s) of Connection are defined in the SIA. See paragraph 4.25 below.

⁴³ When an emergency call is made on 999 or 112, in order to connect the call to the correct local emergency organisations, the call is first answered by an emergency CHA who, from the information provided from the network and from speaking direct to the caller, is able to forward the call to the correct emergency service at the nearest geographic location to the caller.

the BT Switch Connections that exist at BT exchanges in York, Sheffield and Leeds.⁴⁴

- 4.5 CPs are at liberty to choose the location of the BT Switch Connections that they want to utilise, subject to commercial negotiation and availability. Each CP can also choose how to route calls across its network to these BT Switch Connections, for example by using its own infrastructure to take traffic to the Switch Connection directly or by contracting this function to a third party.
- 4.6 How KCOM routed its emergency call traffic to the BT Switch Connections at York, Leeds and Sheffield is particularly relevant to this investigation and we consider this further below.

KCOM's emergency call routing

- 4.7 At the time of the incident, KCOM routed its emergency call traffic via two KCOM Switch Connections at [REDACTED] KCOM location 1] and [REDACTED] KCOM location 2] to the BT Switch Connections at York, Sheffield and Leeds. It is at these [REDACTED] locations that KCOM's network and BT's network interconnected and where traffic could be switched onto the BT PSTN network for onward routing to the CHA. The high-level architecture of the interconnection between KCOM and BT's network is shown in Figure 1.

Figure 1: [REDACTED]

[REDACTED]

- 4.8 KCOM used multiple circuits between the Switch Connections in an attempt to ensure location and route diversity for its emergency calls (i.e. that a failure of an individual route or location would not lead to a failure of the overall service). Each Switch Connection could support multiple telephone calls.

⁴⁴ The BT exchanges at York, Sheffield and Leeds are BT Digital Main Switch Units ('BT DMSUs') or BT Next Generation Switches ('BT NGSS') that form part of BT's nationwide core telephone network.

- 4.9 To implement the architecture in Figure 1, KCOM provisioned its own infrastructure to provide primary capacity. Specifically, KCOM used its own infrastructure to connect its [§< KCOM location 1] and [§< KCOM location 2] Switch Connections to the BT Switch Connection at York, creating two discreet traffic routes.
- 4.10 In order to provide back-up capacity if something were to go wrong on its primary routes to the BT Switch Connection at York, KCOM procured the use of additional circuits from BT to take its traffic to the BT Switch Connection at York, as well as to alternative nearby BT Switch Connections at Leeds and Sheffield.
- 4.11 [§< Several] routes were used, connecting the two KCOM Switch Connections at [§< KCOM Location 1] and [§< KCOM location 2] with the three BT Switch Connections at York, Leeds and Sheffield. For each route, multiple [§<] circuits were provided. In total [§< many] individual BT-provided [§<] circuits were used to access the BT Switch Connections at Leeds, York and Sheffield. These circuits were already in place at the time and were used as ingress routes by BT to take voice call traffic from its network to the KCOM network.
- 4.12 In respect of the [§< many] BT circuits that represented the back-up capacity, BT used its existing transmission (SDH) network to provide the necessary capacity. While BT had SDH infrastructure at York, Sheffield and Leeds, it had none at [§< KCOM location 2] or [§< KCOM location 1]. Therefore, KCOM used its own infrastructure to bring capacity to a location just outside two BT exchanges at [§< BT location 1] and [§< BT location 2] and used what is termed 'In-span Interconnect ('ISI') (explained further in paragraph 4.34 below) to connect its transmission equipment with that of BT by directly connecting individual fibres together.
- 4.13 In this way circuits were provided between [§< KCOM location 2] and [§< KCOM location 1] to two BT SDH nodes at [§< BT location 1] and [§< BT location 2] using KCOM's infrastructure after which the BT SDH network was used. The nodes at [§< BT location 1] and [§< BT location 2] would therefore have been the physical location where KCOM emergency call traffic was handed over to the BT SDH network however as BT did not offer Switch Connections at these exchanges, the intention was for the emergency call traffic to be routed on the individual BT circuits to the BT Switch Connections at York, Leeds and Sheffield. From the Switch Connections, the emergency call traffic could be switched onto the BT PSTN network for onward routing to the CHA.
- 4.14 Figure 2 shows how BT's SDH network was used to provide capacity in conjunction with KCOM's own network. The dashed lines represent the primary connections provisioned by KCOM.

Figure 2: [REDACTED]

[REDACTED]

[REDACTED]

- 4.15 Again, at this high-level, it appears that both route and node diversity were provided through the SDH network as multiple connections were established between [REDACTED BT location 1] and [REDACTED BT location 2] and the BT Switch Connections at York, Sheffield and Leeds.
- 4.16 However, Figure 2 only shows the end-points between connections, not the individual routes used to carry KCOM's emergency call traffic between those end-points. The individual routes are shown in Figure 3 below.

Figure 3: [REDACTED]⁴⁵

[REDACTED]

[REDACTED]

- 4.17 Of the [REDACTED many] individual circuits provisioned over BT's SDH network to BT's Switch Connections, [REDACTED most] were routed to, or through, the York Stonebow exchange [REDACTED]⁴⁶. The [REDACTED few] remaining circuits that did not pass through York were from [REDACTED BT location 1]: [REDACTED some] were routed to, and terminated at, Sheffield whereas the other was routed to Sheffield and from there routed to, and terminated at, Leeds.
- 4.18 When the York exchange was compromised due to flooding, KCOM's primary connections failed as did the [REDACTED] protection circuits routed over BT's SDH network. Moreover, the signalling associated with the [REDACTED few] paths that avoided York was routed via the BT York Stonebow exchange. This meant that the [REDACTED few] remaining circuits could not be utilised for carrying traffic, leading to what BT described as "... a *total interdependency on York*".⁴⁷ Consequently, the failure of the York exchange caused the complete failure of all emergency calls from the KCOM area.
- 4.19 In summary, therefore, at the time of the Incident the BT York Stonebow exchange constituted a single point of failure for all circuits used for the conveyance of KCOM emergency call traffic, either due to the physical routing of circuits or through the loss of signalling necessary to utilise alternative routes.

⁴⁵ [REDACTED]

⁴⁶ [REDACTED]

⁴⁷ BT's Second Response, Question 1.

KCOM's contractual arrangements

The SIA

- 4.20 The SIA is a standard contract that BT has in place with each of the CPs which interconnect with BT in order to pass traffic across the BT network. BT signs a separate SIA with each CP, although the terms and conditions of each SIA are identical. KCOM and BT originally signed the SIA on 24 January 1997.⁴⁸
- 4.21 KCOM contracted with BT on 19 December 2008 to provide for KCOM's use of BT's CHA services.⁴⁹ This led to an amendment to the SIA to include Schedule 225 of Annex C, which took effect on 25 February 2009.
- 4.22 Schedule 225 sets out BT's general obligations in relation to the provision of access to its CHA services. Annex A to the SIA also sets out the parties' obligations and responsibilities in relation to establishing interconnect links and traffic routes between the BT System and the KCOM System as well as responsibilities relating to ensuring route diversity.
- 4.23 We set out below the relevant provisions as well as the definitions (as set out in the SIA) associated with these various connection points and interconnect links.

The Point of Connection

- 4.24 Clause 4 of Schedule 225 sets out "BT's General Obligations" in relation to emergency call traffic. It requires that, subject to the provisions of Schedule 225, BT shall, amongst other responsibilities, *"where Emergency Calls are handed over at agreed Points of Connection"*:
- convey emergency calls to a CHA;⁵⁰
 - provide an onward connect service for such calls to the relevant emergency service via a BT operator by means of two-way telephony;⁵¹
 - convey all emergency calls handed over by KCOM at all times and at the same standard and quality of service as BT provides to its customers;⁵² and
 - correct faults which occur in the BT network and which affect emergency calls handed over by KCOM in accordance with BT's normal engineering practice. BT does not warrant that its network is or will be free from faults.⁵³
- 4.25 A Point of Connection is defined in Annex D to the SIA as *"a physical point where the BT System and the Operator System are connected for Calls to be handed over from one System to the other"*.

⁴⁸ KCOM's First Response, Question 5.

⁴⁹ Prior to February 2009, KCOM provided its own emergency call handling and routing function using its own CHA located in KCOM premises in Hull and therefore calls by KCOM customers to the emergency organisations were routed exclusively on the KCOM network (KCOM First Response, Question 3).

⁵⁰ Clause 4.1.1, Schedule 225 to Annex C of the SIA. See Annex 12.

⁵¹ Clause 4.1.2, Schedule 225 to Annex C of the SIA. See Annex 12.

⁵² Clause 4.2, Schedule 225 to Annex C of the SIA. See Annex 12.

⁵³ Clause 4.3, Schedule 225 to Annex C of the SIA. See Annex 12.

- 4.26 Under paragraph 5.7 of Annex A to the SIA, parties are required to maintain a record of the physical arrangements for traffic routes in the form of a Technical Master Plan. KCOM has supplied a copy of the Technical Master Plan which sets out the agreed Point(s) of Connection between KCOM and BT as being York, [✂ BT Location 1] and [✂ BT Location 2].⁵⁴

BT Switch Connection

- 4.27 Schedule 225 also sets out the “Operator’s General Obligations” in relation to emergency call traffic. Clause 5.1 specifies that “*where the Operator delivers an Emergency Call to the BT System it shall do so at an agreed BT Switch Connection in accordance with Annex A, and shall conform with the other requirements for Emergency Calls set out in Annex A*”.

- 4.28 A BT Switch Connection is defined in Annex D to the SIA as:

“a BT Exchange at which Calls handed over:

(a) from the Operator System are initially switched; or

(b) to the Operator System are finally switched;

by BT;”

- 4.29 Annex A to the SIA sets out the provisions for the use of BT Switch Connections in relation to all call traffic. At paragraph 4.1.1 it states that:

“The Operator shall nominate by written notice to BT, the BT Switch Connections at the following BT Exchanges identified in accordance with paragraph 3.1 (where the Operator wishes to handover Calls from the Operator System to the BT System):

(a) Any BT Tandem Exchange;

(b) Any BT DLE;

(c) Any BT ISC.”

- 4.30 Appendix 24D,⁵⁵ which is associated with Schedule 225 and BT’s Interconnect Provisioning Manual,⁵⁶ states:

“Operator Services Calls handed over from the Operator System to the BT System shall be at agreed BT Switch Connections. Those BT Switch Connections where such calls are handed over from each appropriate Operator Switch Connection are shown in this table.

⁵⁴ “KCOM_Transmission.xlsx’ provided by KCOM in its response to Ofcom’s second information request indicates [✂ BT location 2] and [✂ BT location 1] as Points of Connection.

⁵⁵ Appendix 24D was provided at Annex 2 of KCOM’s First Written Response. In KCOM’s Second Response, Question 4, KCOM explained that “Appendix 24D is one of the appendixes to BTW’s Standard Interconnect Agreement. Appendix 24D...its central purpose is to identify the traffic routes for emergency calls”.

⁵⁶ See <https://www.btwholesale.com/pages/static/help-and-support/product-documentation.htm>.

IT SHOULD BE NOTED THAT OPERATOR SERVICES CALLS MAY NOT BE DELIVERED INTO THE BT NETWORK AT DJSUs, WATs, DLTEs or DLEs, THESE CALLS MUST BE DELIVERED AT NGSs/DMSUs.”⁵⁷

4.31 Both the Capacity Profile⁵⁸ and Appendix 24D to the SIA⁵⁹ agreed between KCOM and BT specify that the BT Switch Connections are York, Sheffield and Leeds.⁶⁰ Specifically, Appendix 24D sets out the location of the BT Switch Connections that KCOM chose for the conveyance of its emergency call traffic from the [X KCOM location 2] and [X KCOM location 1] exchanges. It sets out the First Choice BT Switch as “York Ebor DMSU”, the Second Choice BT Switch as “Leeds Turquoise NGS (LS/ADB)”, and the Third Choice BT Switch as “Sheffield Sapphire NGS”.

4.32 Annex A of the SIA also provides in relation to the handover of KCOM’s emergency calls to the BT System⁶¹:

“The handing over of Emergency Calls to the BT System at agreed BT Tandem Exchanges is subject to the following conditions:

(1) Trunk reservation, physical separation or other appropriate method shall ensure the availability of emergency circuits to carry Emergency Calls in the Interconnect Link;

(2) The BT Switch Connection at the BT Tandem Exchange shall route Emergency Calls to the BT Operator. Alternative routing shall be applied by the BT System when required and where this alternative routing fails, the BT System shall return a terminal congestion indication to the Operator;

(3) Where possible, the Operator System shall present the relevant BT Tandem Exchange with an Initial and Final Addressing Message (“IFAM”) containing the protection bit set.”⁶²

Interconnect Links and Traffic Routes

4.33 Paragraph 5.2.1 of Annex A to the SIA specifies that “...the Parties shall establish Interconnect Links to convey Calls between the BT system and the Operator System on Traffic Routes between each Operator Switch Connection and at least one BT DMSU”.⁶³

⁵⁷ Appendix 24D, comment attached to “First Choice BT Switch” in tab 24D-G. KCOM also referred to this in the KCOM Second Response, Question 5, where it sets out that “Appendix 24D details the BT Switch Connections that were in place when the February 2009 SIA was signed between BT and KCOM and have remained unchanged over the intervening period”.

⁵⁸ ‘KCOM_Capacity Profile.xlsx’ provided by KCOM in its response to Ofcom’s second information request.

⁵⁹ ‘KCOM_999_Operator Services_Routing Plan.xlsx’ provided by KCOM in its response to Ofcom’s second information request.

⁶⁰ We note here that the Points of Connection of [X BT location 1] and [X BT location 2] are not NGSs or DMSUs. ⁶¹ The BT System is defined in Annex D to the SIA as “the Public Electronic Communications Network provided by BT for connection to the Operator System pursuant to this Agreement”.

⁶² Clause 18.5, Annex A to the SIA. See Annex 13.

⁶³ Annex D of the SIA, page 16. See Annex 20.

- A Traffic Route is defined as “discrete and identifiable units of 2Mbit/s Capacity within an Interconnect Link”.
- An Interconnect Link is defined as “a Link connecting a BT Switch Connection and an Operator Switch Connection passing through a Point of Connection”.

- 4.34 We asked KCOM for any schedules to the SIA or any other agreements with BT that set out the arrangements that it had in place as to how [X BT location 1] and [X BT location 2] were to be used for the conveyance of emergency call traffic in the event that this back-up capacity was required. KCOM stated that “*At the time of agreeing the hand- offs using the SIA both KCOM and BT would have agreed to the locations and type of ISI and then built their respective part*”.⁶⁴ It referred to Schedule 01 to Annex C of the SIA which sets out terms relating to In span Interconnect (ISI) which is the “*provision jointly by each Party of an Interconnect Link by the provision of an ISI Interconnect Link and 2Mbit/s ISI Interconnect Links, such Link having its Point of Connection on the public highway or, subject to the Parties’ agreement, on a prospectively maintainable public highway, with portion of the Interconnect Link being provided by each Party on its side of the Point of Connection*”.⁶⁵
- 4.35 BT also referred to the “*agreement*” that it had with KCOM that, in the event of a failure on the primary route for KCOM emergency call traffic to the point of interconnect (or Switch Connection as it is referred to in the SIA) at the BT York Stonebow exchange, KCOM’s emergency calls would be handed over onto existing BT ingress routes for onward routing to the BT Switch Connections at the exchanges in York, Leeds and Sheffield. BT told us that the “*agreement*” referred to the fact that “*BT and KCOM agreed, either formally or informally that certain routeing can be used*”.⁶⁶
- 4.36 We requested written evidence of this agreement from BT. BT told us that it did not have any written record of the agreement and that it “*may have been made verbally between the account manager at the time and KCOM*”. BT explained that “*this agreement pre-dated the current account manager and was also before the contract was managed by BT MSL. The person that would have been responsible has since left the company.*”⁶⁷

Interconnect Route Diversity and Security

- 4.37 In relation to interconnect route diversity and security, the SIA provides:

*“Where either Party requests physical route diversity it shall take account of the Signalling Links and the Traffic Routes.”*⁶⁸

*“The Traffic Route(s) between an Operator Switch Connection and the relevant BT Switch Connection shall, subject to the normal planning practices of the relevant Party, ensure that a single failure of equipment does not give rise to failure of a Traffic Route.”*⁶⁹

⁶⁴ KCOM’s Second Response, Question 3.

⁶⁵ Clause 2.3, Schedule 01 to Annex C of the SIA. See Annex 21.

⁶⁶ BT’s Fourth Response, Question 1.

⁶⁷ BT’s Fourth Response, Question 2.

⁶⁸ Annex A to the SIA, paragraph 5.5.1. See Annex 13.

⁶⁹ Annex A to the SIA, paragraph 5.5.2. See Annex 13.

- 4.38 More generally, in relation to the interconnection of their networks, KCOM and BT have agreed to “*develop and apply network traffic management strategies and procedures to maintain customer service quality...*” which are to include “*designation of specific Traffic Routes to restore service if a route loss occurs*”.⁷⁰
- 4.39 The SIA also allocates responsibility for different call types to BT and/or KCOM with respect to issues such as the choice of BT Switch Connections and the provision of capacity within the link connecting a BT Switch Connection and a KCOM Switch connection. With respect to emergency traffic from KCOM to BT such responsibility is allocated to KCOM.⁷¹

The Horizon contract

- 4.40 KCOM also agreed a separate contract with BT MSL in June 2009 in relation to the operation and management (but not ownership) of all aspects of KCOM's network in Hull, as well as responsibilities in relation to KCOM's national network. This contract is known as the “Horizon contract”.⁷²

- 4.41 KCOM's objectives in entering into the Horizon contract are [X]:

*“KCOM is seeking to obtain managed network services in respect of its Hull network and national network and to transform its national network offering to enable it to provide “next generation” services and products to its customers using the Supplier's Next Generation Network.”*⁷³

- 4.42 The obligations of BT MSL and KCOM under the Horizon agreement include those summarised in the following paragraphs.

Terms relating to BT MSL's responsibilities

- 4.43 [X] the Horizon contract stipulates that BT MSL provides a number of services to KCOM. These include the provision of the “Hull Managed Services”, [X] as follows:

*“[BT MSL] is responsible for designing, planning, monitoring, maintaining, operating and managing all aspects of the KCOM Hull Network indicated as Supplier responsibilities[X]....ensuring that all such aspects of the KCOM Hull Network are available for use by KCOM and all KCOM Customers 24 hours a day 365 days a year”.*⁷⁴

⁷⁰ Clause 5.1.2, Annex A to the SIA. See Annex 13.

⁷¹ Clause 5.1.3, Annex A to the SIA. See Annex 13.

⁷² [X]

⁷³ [X]

⁷⁴ [X]

4.44 [REDACTED] sets out, [REDACTED], the allocation of responsibilities between KCOM and BT MSL in relation to specified elements of the KCOM network.⁷⁵

4.45 [REDACTED]

4.46 [REDACTED]

4.47 [REDACTED]

4.48 [REDACTED]

4.49 [REDACTED]⁷⁶

4.50 [REDACTED]

4.51 [REDACTED]⁷⁷

⁷⁵ A copy of the Demarcation Diagram can be found at Annex 22.

⁷⁶ [REDACTED]

⁷⁷ [REDACTED]

Terms relating to KCOM's responsibilities

4.52 Under the terms of the Horizon contract KCOM also retains responsibilities and capabilities to audit, review and assess network architectures on its network. [X]

4.52.1 [X]

4.52.2 [X]⁷⁹

4.52.3 [X]

4.52.4 [X]

4.52.5 [X]

KCOM's emergency call risk management

Risk management organisational structure

4.53 KCOM provided us with an organogram in response to our request for information about the teams and/or organs within KCOM responsible for the conveyance of emergency call traffic and the position of each such team and organ within the decision-making structure for issues relating to the conveyance of emergency call traffic.⁸⁰

4.54 [X]

⁷⁹ [X]

⁸⁰ [X]

- 4.55 The organogram also includes a separate structure in relation to BT MSL and its functions under the Horizon contract and notes that “*the emergency call service is managed by BT in a separate agreement*”. No individual or team within KCOM itself is specifically identified on the organogram provided by KCOM as having primary responsibility for, and oversight of, the conveyance of emergency call traffic on KCOM’s network or the emergency call services provided by BT under the SIA. There is also no discrete decision-making structure identified on the organogram in relation to issues relating to the conveyance of emergency call traffic.
- 4.56 As noted in Section 3, Ofcom has previously sought information from KCOM on the measures it was taking to manage cyber security risks. In the March 2014 Letter, KCOM provided Ofcom with information about how it manages security risks generally in relation to its network and services. KCOM explained that its Chief Financial Officer was responsible at board level for security matters and that those with day-to-day responsibility for these matters provided him with regular information about risks and how they are managed by KCOM. [REDACTED]
- [REDACTED]
 - [REDACTED]
- [REDACTED]⁸¹
- 4.57 In KCOM’s Annual Report 2014/15 (the most recent published Annual Report at the time of the Incident), KCOM said that “*Risk management is key to all that we do as a business*” and that “*Risk Management is built into all our processes*”.⁸² It explained that it has a “risk team” which has specific responsibility for a range of risks, including legal risks, governance and all matters relating to standards and compliance.⁸³ It also provided a description of risk management responsibilities within KCOM, stating that the KCOM board is responsible for ensuring that KCOM maintains sound internal controls and risk management systems and that senior managers are responsible for ensuring that all relevant risks are recorded and are being appropriately mitigated within reasonable timeframes.⁸⁴ It said that there are forums for senior management to discuss specific risks and trends and to review the work being done to mitigate any issues.⁸⁵
- 4.58 The Annual Report 2014/15 also included details of the principal risks that KCOM considered faced the business.⁸⁶ These included: (i) the security and resilience of

⁸¹ [REDACTED]

⁸² KCOM Annual report and accounts 2014/15, page 35. See Annex 16.

⁸³ KCOM Annual report and accounts 2014/15, page 35. See Annex 16.

⁸⁴ KCOM Annual report and accounts 2014/15, page 35. See Annex 16.

⁸⁵ KCOM Annual report and accounts 2014/15, page 35. See Annex 16. A “Security Forum” is identified as one of the forums that exist in KCOM for these discussions.

⁸⁶ We have also looked at KCOM’s Annual Reports, which are still publicly available, from 2009/10 – 2015/16. Each of these Annual Reports has identified security and resilience of IT, networks and services as a key risk; customer service and delivery has also been on the list of key risks in each

KCOM's networks and IT systems; (ii) customer service and delivery; and (iii) reliance on key partners and suppliers.⁸⁷ In respect of each of these risks, the Annual Report 2014/15 detailed KCOM's assessment of the risk and the action that KCOM was taking to mitigate it:

- 4.58.1 In relation to network security and resilience, the Annual Report said that it is "essential" to build security and resilience into the networks and systems. To mitigate the risk, the Annual Report recorded that KCOM takes "*action where necessary to ensure we have robust security in place*", complies with security standards and has made significant investment in its infrastructure to improve resilience.⁸⁸
- 4.58.2 In relation to customer service, the Annual Report said that "*delivering exceptional service*" is a key strategic aim. To mitigate the risk, the Annual Report recorded that KCOM invests in people and systems to ensure it has the right people in the right roles with the tools to deliver an exceptional service. It also said KCOM works closely with its partners to ensure that they are aligned with delivering the best service possible.⁸⁹
- 4.58.3 In relation to reliance on key partners, the Annual Report identified BT as one of the key partners that KCOM works with to deliver its services to customers. To mitigate risk, the Annual Report records that KCOM "*monitor[s] all of our partnerships closely to ensure that our partners embody our key values and we can work together to resolve any minor issues before they become significant.*"⁹⁰

Risk assessments and risk planning

- 4.59 On 29 March 2016, in response to a request for "*all reports, risk assessments, internal and external audits received or carried out by, or on behalf of, KCOM in relation to the routing and/or conveyance of emergency call traffic since 1 March 2011*"⁹¹, KCOM said that since that date no specific risk assessments had been carried out by, or on behalf of, KCOM solely in relation to the routing and/or conveyance of emergency calls (other than the root call analysis of the Incident).⁹² However, it attached "*for completeness*" documents that "*show the low level risk assessments related to the transmission networks and the [3<]switching networks, which concern all forms of Time Division Multiplexing (TDM) call conveyance for the last three years.*"⁹³
- 4.60 In its Response to the section 96A Notification of 30 June 2017, KCOM provided more information about these "low level risk assessments", explaining that in early 2012 it initiated a project to produce a "Business Continuity Management System" (BCMS) to "*ensure that there were appropriate business continuity and disaster*

Annual Report since 2012/13. Reliance on third party suppliers was identified as a key risk in each of the Annual Report, other than the last for 2015/16, where it was downgraded as a risk which is "*simply part of the risk of doing business*".

⁸⁷ KCOM's Annual report and accounts 2014/15, pages 20 and 21. See Annex 17.

⁸⁸ KCOM's Annual report and accounts 2014/15, page 20. See Annex 17.

⁸⁹ KCOM's Annual report and accounts 2014/15, page 21. See Annex 17.

⁹⁰ KCOM's Annual report and accounts 2014/15, page 21. See Annex 17.

⁹¹ Ofcom's 11 March 2016 information request to KCOM, Question 8.

⁹² KCOM First Response, Question 8.

⁹³ KCOM First Response, Question 8.

recovery plans for KCOM's core networks and for BT MSL's managed services".⁹⁴

KCOM explained that there were 15 risk assessments undertaken during the BCMS in relation to the elements of the KCOM network that were considered critical to support voice services.⁹⁵

- 4.61 These risk assessments related to KCOM's own network infrastructure and did not cover an assessment of risk to the emergency call service as a whole, nor of the BT routes available to be utilised for the conveyance of KCOM emergency call traffic to BT's Switch Connections. KCOM confirmed that this did not include *"individual risk assessments in relation to elements of the BT network that it used (such as the links that failed), since it would not have any access to the information about specific risks, nor the ability to do anything about reconfiguring such elements in the event that a risk was identified."*⁹⁶
- 4.62 KCOM also set out that in 2014 it embarked on a further risk management review, establishing in August 2014 a "[X] Incident Response Plan" which *"created additional layers of disaster planning and risk management that were retained by KCOM while BT continued to undertake its obligations under the Horizon Agreement"*. KCOM provided seven contingency plans produced under the [X] Incident Response Plan for incidents occurring on its network including flood response, widespread power failure and cyber security response plans.⁹⁷
- 4.63 KCOM also explained that a "[X] alarm management system" was in place at the time of the Incident, which *"was monitoring and reporting alarms, alongside traffic capacity management systems"* and that *"alarms were raised when the routes to York Ebor⁹⁸, Sheffield Sapphire and Leeds Turquoise failed"*.⁹⁹

The Incident

- 4.64 As explained above, as at 27 December 2015, KCOM's emergency call traffic was being routed from Hull to the BT York Stonebow exchange. Moreover, the routing associated with the signalling that should have enabled emergency call traffic to be conveyed to the BT Switch Connections at Sheffield and Leeds, also passed through the BT York Stonebow exchange. The loss of this exchange therefore meant that KCOM's emergency call traffic was not transmitted any further and led to the complete failure of KCOM's emergency call service.
- 4.65 The KCOM emergency call service failure lasted from 21:58 on 27 December 2015 until 01:43 on 28 December 2015, a period of 225 minutes. During this period, KCOM end-users were unable to contact the emergency organisations from fixed lines using the numbers 999 or 112.
- 4.66 This affected 187,406 lines¹⁰⁰ and led to 74 customer-attempted emergency calls from KCOM lines that failed. There were 46 repeat calls within this time, where KCOM end-users were unable to contact emergency organisations and made at least

⁹⁴ KCOM's Response to the 96A Notification, paragraph 2.59.

⁹⁵ KCOM's Response to the 96A Notification, paragraph 2.60.

⁹⁶ KCOM's Response to the 96A Notification, paragraph 2.60.

⁹⁷ KCOM First Response, Question 10.

⁹⁸ We understand that the terms 'Ebor', 'Sapphire' and 'Turquoise' refer to specific switching equipment located in the BT exchanges.

⁹⁹ KCOM First Response, Question 9(a).

¹⁰⁰ KCOM has said that this number is likely to inflate the effective line count in the Hull area as it includes Private Branch Exchange (PBX) lines.

one further attempt. One customer attempted eight calls in the period between 22:47 on 27 December 2015 and 01:42 on 28 December 2015, before eventually getting through at 02:12 on 28 December 2015.¹⁰¹

4.67 [redacted]¹⁰² [redacted]¹⁰³

KCOM actions in response to the Incident

Actions taken on the night

- 4.68 As detailed above, KCOM contracted with BT MSL in relation to the operation and management of all aspects of the KCOM network in Hull. As a result of this contract, it was BT MSL who took the initial actions in response to the Incident. We consider that any actions taken by BT MSL in relation to KCOM's network or services were taken on KCOM's behalf.
- 4.69 The sequence of events on the night of 27/28 December 2015 and BT MSL's response to them are set out in a chronology provided in the Report (the Chronology)¹⁰⁴ and a timeline prepared by BT MSL as part of the RCA (the Timeline).¹⁰⁵
- 4.70 The Timeline shows that BT MSL was receiving and responding to flood alerts and warnings that could impact KCOM's telecoms services throughout the day on 27 December 2015. This included responding to alarms received in the [redacted alarm management] system, as well as despatching engineers to investigate and rectify issues.¹⁰⁶
- 4.71 According to the Chronology, there was a Government notification at 21:43 on 27 December 2015 that the BT York Stonebow exchange was flooding and that asked CPs to let the Department for Culture, Media and Sport know if they were affected by the flood by 09:30 the following day. The Timeline indicates that BT MSL was informed at 22:48 by the BT Major Incident team that the BT York Stonebow exchange had failed.¹⁰⁷ This is confirmed by a log update embedded in the Chronology, in which [redacted] recorded at 22:48:32 that she had spoken to

¹⁰¹ The Report, Annex 2.

¹⁰² [redacted]

¹⁰³ [redacted]

¹⁰⁴ The Report, Annex 1, pages 6 to 9.

¹⁰⁵ The RCA, attachment to paragraph 5.4 titled "27th December 2015 Time line". A copy is available at Annex 11.

¹⁰⁶ The RCA, attachment to paragraph 5.4 titled "27th December 2015 Time line", pages 1 and 2.

¹⁰⁷ The Report, Annex 1, page 3.

BTNet, *“who advised that there is a major Network incident at York due to the flooding”*.¹⁰⁸

- 4.72 A call log annexed to the Report reveals that the first KCOM emergency call failure was at 21:58 on 27 December 2015.¹⁰⁹ However, according to the Timeline, it was not until 23:42 that the emergency call service failure became known to BT MSL. This was alerted to them by the Humberside Police who reported that they were receiving no incoming emergency calls.¹¹⁰
- 4.73 It was following this call from Humberside Police that BT MSL engineers made test calls from the KCOM network and found that *“all test calls received the emergency announcement but never mature to an operator and subsequently cannot be put through to the emergency authority”*.¹¹¹
- 4.74 At this point, BT MSL engineers analysed the *“complex route data configurations to identify why emergency calls were failing...”*.¹¹² Engineers were subsequently able to identify an additional route for the emergency call traffic that went via the [X KCOM Location 1] exchange to the [X KCOM Location 3] exchange. Using this route, the emergency call service was restored by 01:43 on 28 December 2015.¹¹³

KCOM subsequent actions

- 4.75 Immediately following the Incident, KCOM held discussions with BT to ensure that appropriate resilience was put in place for the point of interconnect at the BT York Stonebow exchange. KCOM said it had *“retained resilience using fibres from our national network until such a time as we are assured that BT has put in place the requisite diversity to effectively support 999 services originating from our network in Hull”*.¹¹⁴ KCOM also explained that it was conducting an *“internal audit of all points of interconnection”* and had additionally *“asked BT to do an independent audit of all our network and interconnect arrangements to ensure resilience”*.¹¹⁵
- 4.76 The RCA was undertaken by BT MSL on KCOM's behalf and set out the reason for the KCOM emergency service failure as well as making recommendations and proposing actions moving forward. BT MSL stated in the RCA that it had *“implemented all of the recommendations within the actions in this report”*.¹¹⁶
- 4.77 BT MSL explained in the RCA that it had reviewed the physical routing for emergency calls both outbound and inbound to the City of Hull and had taken steps to ensure that there was no longer a single point of failure in the transmission of emergency calls. Specifically, the transmission routes that serve the Leeds and Sheffield ingress routes to Hull were rearranged, moving these principal routes away

¹⁰⁸ A copy of the log update that is embedded in the chronology at Annex 1 of the Report (at the 22:00 entry) is available at Annex 14.

¹⁰⁹ The Report, Annex 2, page 12.

¹¹⁰ The RCA, attachment to paragraph 5.4 titled *“27th December 2015 Time line”*, page 3.

¹¹¹ The RCA, attachment to paragraph 5.4 titled *“27th December 2015 Time line”*, page 3.

¹¹² The RCA, attachment to paragraph 5.4 titled *“27th December 2015 Time line”*, page 3.

¹¹³ The Report, Annex 2 confirms that an emergency call was successfully connected at 01:43 on 28 December 2015.

¹¹⁴ The Report, paragraph 21.

¹¹⁵ The Report, paragraph 21.

¹¹⁶ The RCA, section 4.7. The actions are listed in section 4.6 of the RCA and we note, in particular, actions 001, 002 and 003 in relation to the diversity of the route options for KCOM emergency call traffic.

from the BT York Stonebow exchange to other areas of the BT network in East Yorkshire.¹¹⁷

- 4.78 BT provided details of the current transmission routes for conveying KCOM emergency call traffic that were commissioned following the Incident.¹¹⁸ This information shows that while the routes between KCOM and the BT York Stonebow exchange are unchanged from those prior to the Incident, in the new architecture none of the routes to Sheffield and Leeds pass through the BT York Stonebow exchange.
- 4.79 The RCA also noted that, following the Incident, BT MSL made improvements to the record management and alarm systems used for KCOM emergency call traffic. It noted that a detailed set of records and network drawings had been updated to reflect the current network configuration and that these can be accessed by the operational team members in the event of a future incident. In addition, it explained that the “[redacted]resources confirmed as carrying emergency call traffic have been “labelled” within the [redacted]alarm handling platform to ensure that any loss of associated “emergency service resource” is clearly highlighted within the NMC^[119] monitoring screen”.¹²⁰
- 4.80 KCOM also confirmed that, following the Incident, [redacted KCOM’s alarm management system] “monitoring improvements have been implemented to improve monitoring and response times to circuits that route emergency calls” and confirmed that “[a]ll Hull sites have had their [redacted]signalling links tagged as carrying emergency traffic within [redacted the alarm management system]”. It said that this now enables the engineers to “identify, triage any failures which could impact emergency calls more efficiently and then follow the correct reporting process for Emergency Authorities...”.¹²¹
- 4.81 In addition, the RCA explained that an incident management review that was undertaken following the Incident led to an updated process for the NMC to follow to initiate communications with appropriate emergency authorities and that training was rolled out to NMC members regarding awareness and operational use of the process.¹²²
- 4.82 Finally, BT MSL has said that “all future network configurations for critical services, such as the 112/999 service will be planned and reviewed with an associated risk assessment to eliminate single points of failure for all disciplines (switch, transmission, etc.)”. [redacted]¹²³

D

¹¹⁷ RCA, paragraph 3.5.2.

¹¹⁸ BT First Response, Question 4.

¹¹⁹ BT MSL’s Network Management Centre.

¹²⁰ RCA, paragraph 3.4.2.

¹²¹ KCOM First Response, Question 9(b).

¹²² RCA, paragraph 3.4.3.

¹²³ [redacted]

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 KCOM 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 from 26 May 2011 to 28 December 2015.

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 would 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 obligations to take all necessary measures to maintain, to the greatest extent possible, 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 do not consider that KCOM had diverse and resilient emergency call routing in place as there was a single point of failure at the BT York Stonebow exchange. This single point of failure was present throughout the Relevant Period and led to the total failure of KCOM's emergency call service on the night of the Incident.
- 5.5 We consider that there were technically feasible and proportionate actions that KCOM could have taken to have avoided this single point of failure as it had various other routing options available to it that were not dependent on the BT York Stonebow exchange. Using these for the conveyance of KCOM's emergency call traffic for hand over to BT would not have required a resource heavy, complex or costly solution.
- 5.6 We also consider that it would have been in KCOM's reasonable control to have secured this resilience. Whilst KCOM did have a contract in place with BT for the routing of its emergency call traffic on the BT network, we do not consider that it was sufficient for KCOM to have relied on this without taking any further steps to ensure effective diversity.
- 5.7 We consider that there were further reasonable steps that KCOM could, and should, have taken to ensure effective diversity of its emergency call routing. Whilst KCOM has submitted that it did take all of the steps that Ofcom identified in the 96A notification, we remain satisfied that its actions were not sufficient to discharge its obligations under GC3.1(c) for the reasons set out in this Section.
- 5.8 In these circumstances, we consider that there was an ongoing failure by KCOM to secure diverse and resilient routing for this traffic for the duration of the Relevant Period, in breach of its obligations under GC3.1(c).

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

Contravention of GC3.1

5.10 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.

5.11 For the purposes of GC3.1(c), a CP is a person who provides publicly available telephone services. KCOM is therefore subject to the requirements of GC3.1(c) in relation to the telephone services it provides to its customers in Hull.

Approach to assessing compliance with GC3.1(c)

5.12 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 implement “*all necessary measures*” to maintain, “*to the greatest extent possible*”, uninterrupted access to Emergency Organisations as part of their publicly available telephone services.

5.13 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.¹²⁴

5.14 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.

5.15 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*”.¹²⁵

5.16 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

¹²⁴ 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).

¹²⁵ “*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 GC3.¹²⁶

- 5.17 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”.¹²⁷
- 5.18 We also noted¹²⁸ that in 2008, industry, via the Electronic Communications Resilience & Response Group (“EC-RRG”),¹²⁹ 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 these 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.”¹³⁰

- 5.19 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:¹³¹

“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’.”¹³²

¹²⁶ “Changes to General Conditions and Universal Services Conditions”, Statement dated 25 May 2011, paragraph 5.12.

¹²⁷ “Changes to General Conditions and Universal Services Conditions”, Statement dated 25 May 2011, paragraph 5.19.

¹²⁸ “Changes to General Conditions and Universal Services Conditions”, Statement dated 25 May 2011, paragraph 5.13.

¹²⁹ CPs who own or operate key aspects of the telecommunications infrastructure in the UK, including KCOM, are members of the EC-RRG, see <https://www.gov.uk/guidance/telecoms-resilience>.

¹³⁰ “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.

¹³¹ 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.

¹³² “EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure”, March 2008, paragraph 6.2.3.

- 5.20 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.”¹³³

- 5.21 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.
- 5.22 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 there should be diversity in the routing of emergency call traffic wherever possible.¹³⁴ 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.¹³⁵
- 5.23 Given the above, and the circumstances of the Incident, we have considered the following questions in assessing whether KCOM has complied with GC3.1(c):
- 5.23.1 Step 1. Was KCOM's provision of emergency call services sufficiently resilient (including considering whether there was diversity in the emergency call routing)?
- 5.23.2 Step 2. If not, did KCOM take all necessary steps to ensure that the provision of its emergency call service was sufficiently resilient. In particular, would it have been technically feasible¹³⁶ and within KCOM's reasonable control to ensure sufficient resilience was in place?
- 5.24 If we find at Step 1 that the provision of emergency call services was not sufficiently resilient but at Step 2, that it would have been technically feasible and within KCOM's

¹³³ “EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure”, Guidance March 2008, paragraph 7.1.6 (ii).

¹³⁴ 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 5.27 below.

¹³⁵ Also, see paragraphs 5.43 to 5.46 below.

¹³⁶ 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.

reasonable control to ensure sufficient resilience, then Ofcom will consider that there has been a breach of KCOM's obligations under GC3.1(c).

- 5.25 KCOM has an ongoing obligation under GC3.1(c) to ensure routing diversity for emergency call services. A failure which compromises that diversity on an ongoing basis will potentially result in a continuing breach of GC 3.1(c), until that failure is remedied. Accordingly, although the routing for the conveyance of KCOM's emergency traffic was put in place in 2009 (ie before our enforcement powers under section 96C of the Act took effect in May 2011), we have assessed the steps that KCOM could have taken at the stage of designing its routing in order to determine whether it would have been technically possible, and within its reasonable control, to ensure diversity during the Relevant Period.¹³⁷ We nonetheless make no findings as to whether KCOM contravened its obligations under GC3.1(c) during that earlier period.

Step 1: Was KCOM's provision of emergency call services sufficiently resilient?

- 5.26 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 physically and logically diverse emergency call routing in so far as it is possible and proportionate to do so.
- 5.27 In particular, we consider that, in line with industry best practice, CPs should ensure that their emergency call routing 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.¹³⁸ 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 provision of emergency call services (either generally or at specific points within the call routing).
- 5.28 In order to make an assessment of the diversity of KCOM's emergency call routing, bearing in mind the circumstances of the Incident, we have considered the emergency call routing configuration it had in place from its network in Hull up to the BT Switch Connections as at the time of the Incident.
- 5.29 From the information supplied by KCOM, it appears that, at the time of the Incident, it had diverse and resilient routes in place for its emergency call traffic on the KCOM network in Hull. We say this because:
- 5.29.1 KCOM had various routing options available to take its emergency call traffic to its switches at [X KCOM location 2] and [X KCOM location 1];¹³⁹ and
- 5.29.2 The PAC report discusses alternative routing that was available to KCOM, taking calls from its [X KCOM location 4 exchange], [X KCOM location 5 exchange] and [X KCOM location 6 exchange] to KCOM's [X KCOM location 7 exchange] for onward conveyance to BT which could be utilised should an issue occur at both the [X KCOM location 2] and [X KCOM location 1] exchanges.¹⁴⁰

¹³⁷ By virtue of paragraph 13 of Schedule 3 to the Electronic Communications and Wireless Regulations 2011, section 96C of the Act may be applied to a continuing contravention, provided it is not applied in respect of any period of contravention before 26 May 2011.

¹³⁸ See paragraph 5.22 above.

¹³⁹ In making this assessment we have considered the information provided in relation to these routes on the KCOM network in KCOM's First Response, Question 1, as well as the information provided in the PAC Report.

- 5.30 However, we do not consider that KCOM had sufficient diversity in its emergency call routing from its switches at [X KCOM location 2] and [X KCOM location 1] to the BT Switch Connections at York, Leeds and Sheffield. We say this because, both KCOM and BT MSL told us that it became apparent following the Incident that there was an unknown *single point of failure* in the transmission of KCOM emergency call traffic at the BT York Stonebow exchange.¹⁴¹
- 5.31 It appears that KCOM intended to have diversity in this part of its call routing as it contracted with BT for the use of three geographically distinct BT Switch Connections at York, Leeds and Sheffield. This should have provided a good level of diversity as it meant that, in theory, if anything were to go wrong at any one of these three BT Switch Connections, its traffic would be re-routed to one of the other BT Switch Connections for onward routing to the CHA.
- 5.32 However, as detailed in Section 4, the single point of failure existed because of the routes that were chosen to take KCOM emergency call traffic from its switches in [X KCOM location 2] and [X KCOM location 1] to these BT Switch Connections. At the time of the Incident, in order to take its traffic to the BT Switch Connections, KCOM decided to:
- 5.32.1 use its own KCOM egress route to the York Switch Connection. This formed the primary route for its emergency calls and in normal operation this is where KCOM's emergency call traffic was switched over to the BT network for onward routing to the CHA; and
 - 5.32.2 have an agreement with BT to utilise routes on the BT network to provide secondary routes (back-up capacity) to take its traffic to the Leeds and Sheffield Switch Connections in the event of a failure on the primary route, rather than using its own infrastructure to provide this back-up capacity.
- 5.33 As detailed in Section 4, it became clear following the Incident that all circuits that underpinned the BT ingress routes that provided the secondary routes should an issue occur on the route to the BT Switch Connection at York, also had a dependency on the York exchange. As such, both the primary route (to the BT Switch Connection at York) and the secondary routes (to the BT Switch Connections at York, Sheffield and Leeds) were reliant on the York exchange. This routing configuration meant that *"there was a total interdependency on York"*¹⁴² and it represented a single point of failure in KCOM's emergency call routing.
- 5.34 KCOM has not disputed that securing diverse routing is a key aspect of ensuring resilience. It is clear from its submissions that KCOM did in fact seek to put in place diverse and resilient routing for its emergency call services. It remains the case, however, that the routing for the emergency call services that was put in place was not sufficiently diverse as it incorporated a single point of failure.
- 5.35 As such, we do not consider that KCOM had sufficient diversity in its call routing to ensure it could maintain uninterrupted telephone access to the emergency organisations for its end-users. We note that the routing that was in place for

¹⁴⁰ The PAC Report, paragraph 2.2.2.

¹⁴¹ See the Report and the RCA.

¹⁴² BT Second Response, Question 1.

KCOM's emergency call traffic at the time of the Incident was put in place following KCOM's decision to contract with BT for the use of CHA services and the subsequent amendments to the SIA which took effect on 25 February 2009¹⁴³ and there were no substantive changes to this call routing from 25 February 2009 to the date of the Incident.¹⁴⁴ We have therefore inferred that the single point of failure was ongoing from 25 February 2009 and throughout the Relevant Period.

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

- 5.36 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).
- 5.37 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.

Was it technically feasible for KCOM to secure resilience?

- 5.38 When examining technical feasibility, the first question is 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 Switch Connections, or implementing additional risk management actions or processes, such as effective back-up testing, alarm systems and incident management procedures.
- 5.39 In this case, it is clear that it was technically possible to establish a transmission route for KCOM's emergency call traffic which did not pass through or have a dependency on York. Two separate pieces of evidence demonstrate this:
- 5.39.1 KCOM has told us that it had in place its own infrastructure that was not dependant on the York exchange and that could have been utilised to convey calls to the Switch Connection at the exchange in Sheffield;¹⁴⁵ and
- 5.39.2 following the Incident, engineers were able to identify, create and utilise an alternative BT transmission route which bypassed the BT York Stonebow exchange¹⁴⁶ and information received from BT shows that no routes to the BT Switch Connections at Sheffield and Leeds now pass through the BT York Stonebow exchange.
- 5.40 Given that it would have been technically possible for KCOM to have secured from BT or put in place itself a fix, we consider next whether this would have been proportionate in the circumstances, taking into account factors such as complexity, resourcing and cost. Any consideration of proportionality needs to be considered

¹⁴³ KCOM First Response, Question 2.

¹⁴⁴ [38]

¹⁴⁵ As detailed in the PAC Report, paragraph 2.2.2.

¹⁴⁶ RCA, section 3.5.

against the objective of GC3.1(c) – to provide uninterrupted telephone access to the emergency organisations – and the vital public interest that it serves. In saying that, we accept that there may be occasions where such provision would be disproportionate, such as the deployment of protection paths in the access network to all households.¹⁴⁷

- 5.41 In KCOM's case, the issue occurred in a part of the emergency call routing where we would not have expected any single points of failure to arise,¹⁴⁸ and a fix was put in place by engineers within hours of identifying there was an issue in its emergency call routing. This suggests that the issue did not require a resource-heavy or complex solution. KCOM has not made any representations to contend that the costs involved were disproportionately high. We therefore judge that it would have been proportionate for KCOM to have ensured it had sufficient resilience in its emergency call traffic at the outset or at any time up to the Incident.
- 5.42 Accordingly, we conclude that it would have been technically feasible for KCOM to have avoided the single point of failure in its emergency call routing, and to have put in place alternative routing to secure diversity and resilience for these services.

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

- 5.43 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.
- 5.44 The obligations in GC3.1(c) apply to the CP who has the contract with the end-user and that CPs are not able to pass this regulatory obligation to another CP by virtue of any contractual relationship. However, the steps that are proportionate and within a CP's reasonable control in relation to ensuring it has sufficient diversity are likely to vary depending on whether it is establishing routing on its own network, or contracting for the use of routing on a third party network.
- 5.45 For example, where a CP contracts with BT for the use of its CHA services via the SIA, the steps that we would consider proportionate and within a CP's reasonable control once it had handed over its traffic at the BT Switch Connections would differ considerably to the steps we would expect CPs to take to ensure diversity up to this point. This is because:

¹⁴⁷ A CP's access network generally comprises a single line connecting the premises to the local exchange. This link is normally unprotected in that a failure of the cable, duct or telegraph pole between the premises and the exchange would render impossible calls supported by this infrastructure. This architecture is prevalent in most telecoms networks both in the UK and around the world.

¹⁴⁸ By this we mean that the single point of failure existed in a part of the call routing comprising exchange buildings connected by optical fibre links. Buildings contain electronic switching and routing equipment as well as transmission equipment to send signals to other exchanges in the CP's network. This part of the network normally enjoys high levels of protection and resilience, as multiple routes to multiple destinations can be deployed to ensure route and location (node) diversity.

- 5.45.1 Once calls have been handed over to BT at the BT Switch Connections and accepted into BT's network they will be mixed with calls from other CPs as well as BT's own calls. We consider that it would be highly inefficient for all CPs that contract with BT for the delivery of emergency calls to conduct identical audits of network assurance for which BT would be expected to conduct for its own traffic. BT is best placed to manage calls within its network as it needs to manage all emergency calls from all sources in the most efficient manner – making exceptions at the behest of individual CPs could lead to inefficiencies or unforeseen consequences that could lower the quality of the overall service.
- 5.45.2 On the other hand, network infrastructure provision up to the BT Switch Connections, including the choice of the end-points, capacity and routing would be specific to the CP. In these circumstances, it would be possible and proportionate to expect that the CP conducts the necessary checks to ensure they are fit for purpose.
- 5.46 This does not mean that a CP is not required to conduct an assessment of risk when passing its traffic over to BT at BT Switch Connections. CPs should consider and manage the risks associated with any decision to purchase BT's CHA services in fulfilling their obligations under GC3.1 (c). However, as noted, these obligations are applied proportionately, taking account of costs and technical constraints, and this will determine the nature and level of scrutiny which is possible and appropriate in such risk assessments.
- 5.47 As noted at paragraphs 5.32 and 5.33 above, the lack of diversity in KCOM's call routing occurred *before* the emergency calls were switched onto the BT network at the BT Switch Connections and stemmed from the choice of BT routes that KCOM utilised to take its traffic to these BT Switch Connections. The network infrastructure in question was specific to KCOM and it was ultimately KCOM's choice as to whether to utilise BT routes to take its traffic to the BT Switch Connections. We note that KCOM had various options available to it, for example utilising its own infrastructure to the Sheffield switch, or contracting this function to a third party. The routes that KCOM was utilising to the BT Switch Connections were implemented by BT to allow KCOM to extend its network to the BT Switch Connections; no other CPs used these routes for the conveyance of emergency call traffic.
- 5.48 We consider therefore that, whilst it may be reasonable to utilise BT routes (or any other CP's routes) to take calls to the BT Switch Connections, in making the decision to do so KCOM was under an active and ongoing duty to do everything in its reasonable control to ensure that any routes being chosen were part of an overall design that ensured diverse and resilient emergency call routing up to the BT Switch Connections.
- 5.49 It is clear that the BT ingress routes that were ultimately chosen did not fulfil the objective of diverse routing (as they were all reliant on the BT York Stonebow exchange creating a single point of failure). Accordingly, we have examined the available evidence to establish whether KCOM did everything within its reasonable control to ensure that these routes were diverse.
- 5.50 In making our assessment, we have taken account of the representations made by KCOM in KCOM's First Written Response and Response to the 96A Notification.
- 5.50.1 In KCOM's First Written Response, KCOM said that entering into the SIA with BT was one of the most important ways that it ensured diversity in

respect of the BT routes that it was utilising for the conveyance of its emergency call traffic as this agreement put the responsibility on BT to ensure route diversity.

- 5.50.2 In its Response to the 96A Notification, KCOM identified the measures it took in entering into, and implementing, the Horizon agreement with a view to securing network resilience and diversity as demonstrating that it took all steps within its reasonable control.
- 5.51 Taking account of these submissions, our assessment of whether it was within KCOM's reasonable control to ensure resilience is structured as follows:
- 5.51.1 We first consider what responsibilities BT had for route diversity under the SIA, and whether these were sufficient for KCOM to have relied upon to ensure the diversity of the routing for its emergency call traffic;
- 5.51.2 We then consider what further steps, outside the SIA, KCOM could reasonably have taken in order to ensure route diversity; and
- 5.51.3 Finally, we consider KCOM's arguments that it took these (or other similar) steps to ensure the diversity of its emergency call routing.
- 5.52 KCOM has also made submissions about BT's regulatory responsibilities and that Ofcom's provisional view in the 96A Notification was clouded by "hindsight bias". These representations and our response are set out at paragraphs 5.111 to 5.115 below.

BT's responsibilities for route diversity under the SIA

- 5.53 In KCOM's First Written Response, KCOM explains that it was the signalling links on the BT ingress routes that ultimately did not provide the resilience that KCOM anticipated would be available if the primary route to the point of interconnect at York failed and that:

*"KCOM and BT both would have understood that BT was under binding obligations of its own (both under the SIA, and in 2009, under GC3.1(c)) to avoid a single point of failure in its network. As a matter of fact, the 'measures' adopted by KCOM for the purposes of compliance with GC3.1(c) included, in effect, to rely on BT's performance of those obligations."*¹⁴⁹

- 5.54 KCOM also goes on to explain that *"as its name implies, the SIA sets out the industry's standard terms. In relation to emergency call conveyance in particular, Schedule 225 presents not only what a reasonable carrier would have done in KCOM's position when procuring conveyance, but also what every other carrier who purchased equivalent services from BT did in fact do."*¹⁵⁰ KCOM also noted its view that *"properly understood, the most significant single 'measure' that it took to ensure uninterrupted access to the emergency calls access during the period under investigation was to enter into the SIA"*.¹⁵¹

¹⁴⁹ KCOM's First Written Response, paragraph 3.17.

¹⁵⁰ KCOM's First Written Response, paragraph 3.28(b).

¹⁵¹ KCOM's First Written Response, paragraph 5.21.

- 5.55 KCOM pointed us to a number of provisions in the SIA which mean, in its view, that *“BT was, in substance, responsible under the SIA for the planning and design of the routing of KCOM’s emergency call traffic for handover to BT, at least insofar as it relates to BT’s side of the point of interconnection”*.¹⁵²
- 5.56 KCOM referred in particular to paragraph 2 of Schedule 225, which sets out BT’s obligation to convey and hand over emergency calls to a CHA. It also pointed us to paragraph 4 of that Schedule, which sets out BT’s responsibilities in relation to emergency calls handed over *“at agreed Points of Connection”*¹⁵³, and paragraph 5, which stipulates that *“where [KCOM] delivers an Emergency Call to the BT System it shall do so at an agreed BT Switch Connection”*¹⁵⁴.¹⁵⁵
- 5.57 In addition, KCOM referred to a number of provisions of Annex A, including:
- 5.57.1 paragraph 5.5 which provides that:
- “the Traffic Routes between [KCOM’s] Switch Connection and the relevant BT Switch Connection shall, subject to the normal planning practices of the relevant Party, ensure that a single failure of equipment does not give rise to a failure of a Traffic Route”*
- 5.57.2 paragraph 18.5 which states that:
- “the BT Switch Connection at the BT Tandem Exchange shall route Emergency Calls to the BT Operator. Alternative routing shall be applied by the BT System when required and where this alternative routing fails, the BT System shall return a terminal congestion indication to the Operator”*.
- 5.58 Having considered these provisions within the context in which they operate and the requirements of GC3.1(c), we consider that KCOM’s arguments may have been valid had the single point of failure existed after its emergency call traffic had been switched onto the BT network at the BT Switch Connections. However, the single point of failure existed prior to the calls being switched onto the BT network at the BT Switch Connections. As a result of this distinction, we do not consider that these terms demonstrate that KCOM took all necessary steps within its reasonable control to maintain access to the emergency organisations.
- 5.59 First, on an objective assessment of the contractual provisions highlighted by KCOM, we do not consider it was reasonable for KCOM to treat BT as responsible for securing and maintaining the diversity and resilience of its routing for the conveyance of emergency call traffic by means of the routes from the Points of Connections at [X BT location 2] and [X BT location 1] up to the BT Switch Connections at York, Leeds and Sheffield. In particular, we note that:
- 5.59.1 Although paragraph 4 of Schedule 225 of the SIA refers to BT’s responsibilities for traffic handed over at Points of Connection (which include for the purposes of the SIA generally, the points in [X BT Location 2] and [X BT location 1]¹⁵⁶), KCOM’s obligation, in accordance with paragraph 5 of the

¹⁵² KCOM’s First Written Response, paragraph 5.15.

¹⁵³ Schedule 225 of Annex C to the SIA, paragraph 4.1.

¹⁵⁴ Schedule 225 of Annex C to the SIA, paragraph 5.1.

¹⁵⁵ KCOM’s First Written Response, paragraph 5.21.

¹⁵⁶ See paragraphs 4.24 to 4.26 above.

same Schedule, is to deliver emergency traffic at an agreed BT Switch Connection. The agreed BT Switch Connections are identified specifically in relation to KCOM's emergency call traffic in Appendix 24D and the Capacity Profile as the York, Leeds and Sheffield exchanges.¹⁵⁷

- 5.59.2 The obligation in paragraph 5.5 of Annex A of the SIA to ensure that a single point of failure does not occur in a Traffic Route between a KCOM Switch Connection and a BT Switch Connection is said to be subject to the *"planning practices of the relevant Party"*. As set out, paragraph 5 of Schedule 225 suggests that it is KCOM who bears the responsibility for delivering its emergency traffic up to the York, Leeds and Sheffield exchanges.
- 5.59.3 Paragraph 18.5 relates to alternative routing for the conveyance of traffic beyond the exchanges in York, Leeds and Sheffield, and to the application of alternative routing by BT beyond these points.
- 5.60 Noting that the provisions of paragraph 5 of Schedule 225 and the identification of the BT Switch Connections in Appendix 24D and the Capacity Profile apply specifically in relation to the conveyance of KCOM's emergency call traffic, there is a reasonable view that the handover of its emergency call traffic at [X< BT location 2] and [X< BT location 1], was not covered by the terms of the SIA. This appears to be BT's position; it told Ofcom that the use of these routes was agreed by the parties *"formally or informally"*.¹⁵⁸
- 5.61 At best, noting the conflict between paragraphs 4 and 5 of Schedule 225, the terms of the SIA are ambiguous as regards the obligations of BT in relation to KCOM's emergency call traffic handed over at [X< BT Location 1 and BT Location 2]. In the face of this ambiguity, and given the critical importance of maintaining the secure conveyance of this traffic and the high standard set by the obligation in GC 3.1(c), we consider that KCOM should have taken further steps to ensure that the use of these routes and responsibilities for securing resilience and diversity was clearly defined and understood by both parties.
- 5.62 Second, even if BT did have responsibilities under the SIA in relation to the diversity of the BT ingress routes being utilised to take traffic from [X< BT location 2] and [X< BT location 1] to the BT Switch Connections, we still do not consider that KCOM could rely solely on this without taking any further steps.
- 5.63 We say this because KCOM had specific needs in relation to these routes, particularly that these routes should not go through the York exchange, as this is where the primary Switch Connection existed. Therefore, KCOM did not just require the routes to be diverse from each other, it required diverse routing from the York exchange and, ideally, from the KCOM-provided routes used for the primary connections. The standard terms of the SIA contract do not cover this specific requirement.
- 5.64 For these reasons, whilst we consider the SIA was certainly a necessary and significant measure that KCOM took to ensure it was able to provide uninterrupted access to emergency organisations, we do not think it was sufficient for KCOM to have relied on this in respect of ensuring that the routes between

¹⁵⁷ See paragraph 4.31 above.

¹⁵⁸ See paragraphs 4.35 to 4.36 above

[X BT Location 1 and 2] and the BT Switch Connections at York, Leeds and Sheffield were offering the specific diversity that was needed.

- 5.65 Given this, we consider below whether there was anything further that KCOM could have realistically done to ensure that the routes it was using on the BT network met the overall objectives of its emergency call routing.

Further steps in KCOM's reasonable control

- 5.66 Given that KCOM was choosing to use routes on the BT network to take its traffic to the BT Switch Connections (in the event of a failure on the primary route), we accept that KCOM would not have had the same level of control over the routing as it would have done if it were using its own infrastructure. For example, we are not suggesting that KCOM would have been able to design or build new routes on the BT network to meet its objectives.
- 5.67 However, this was KCOM's emergency call traffic, and it was the one who had specific objectives and requirements for this routing (as well as the one who was subject to strict regulatory requirements). In these circumstances, KCOM needed to do everything within its reasonable control to ensure that these objectives were met. This did not have to mean designing the routing itself, but it does mean that KCOM should have maintained effective oversight to the extent that it could satisfy itself that the BT routes that were being utilised were fit for purpose.
- 5.68 This could have been done in a number of ways. For example, we consider that KCOM could have:
- 5.68.1 Ensured that BT and KCOM engineers worked collaboratively to identify the most suitable routes to ensure that traffic could reach the BT Switch Connections at York, Leeds and Sheffield (should an issue occur on the primary route to York) and which offered the necessary diversity based on KCOM's specific requirements;¹⁵⁹
 - 5.68.2 Provided specifications to BT that set out the particular objectives that were pertinent in this case, to allow BT to implement a corresponding design (or similar), and then confirmed with BT that the routes had the necessary diversity from the York exchange;
 - 5.68.3 Required BT to provide 'as-built' routing information, for its own records. Such information is important to facilitate planned engineering or the deployment of additional network infrastructure, by identifying critical network elements. This is particularly useful when network infrastructure from multiple providers exists in proximity to each other as was the case with KCOM's primary and protection routes; and/or
 - 5.68.4 Asked BT, on a periodic basis, to confirm that the routes had the necessary diversity with regards to KCOM's initial requirements and own infrastructure. In this respect, we acknowledge that where a CP contracts

¹⁵⁹ We note that paragraph 3.21 of KCOM's First Written Response suggests that the initial design of the end-to-end network was a shared, collaborative activity as between BT and KCOM, however paragraph 3.23 notes that *"even with that collaborative activity, each party would have been ultimately responsible for design and planning of the network on its side of the interconnection point."* We note in this context the meaning given to interconnection point[s] by KCOM was the Points of Connection of [X BT Location 1] and [X BT Location 2].

with BT for the provision of network services, it is likely to be reasonable to rely on information that BT provides in relation to risks associated with these services. It remains the case, however, that the CP must make appropriate enquiries of BT in order to discharge its obligation to take all necessary steps available. Depending on the response received from BT, KCOM could then have adapted its risk management activities accordingly.

- 5.69 We consider that these (or other similar) steps were within KCOM's reasonable control (either by completing the actions itself, or by ensuring these actions were taken on its behalf) and would have formed part of a robust overall design, planning and implementation process for KCOM's emergency call routing.
- 5.70 In addition, even if KCOM was not involved in the choice of routes from the outset or did not have access to detailed routing information, KCOM could have made appropriate enquiries of BT - in particular, to confirm that BT had due regard to KCOM's key objectives, and specifically the requirement for the routes to be diverse from the York exchange.
- 5.71 We consider these enquiries were particularly important given that KCOM was aware that the routes that were ultimately chosen were fixed BT ingress routes that were already in existence and that were usually utilised to carry BT originated traffic to Hull for transfer onto the KCOM network. This means that the routes had actually been designed for BT incoming calls onto the KCOM network and therefore not necessarily designed with diversity in relation to emergency call traffic in mind. By using routing that had already been designed for a different purpose (albeit with appropriate end-points at the York, Leeds and Sheffield exchanges), there was a greater risk that the routes would not meet KCOM's specific objectives.
- 5.72 Alternatively, had KCOM found itself in a position where BT could not (or was unwilling to) provide it with sufficient information or assurances about the diversity of its routing, we consider this should have prompted KCOM to reconsider its decision to use BT's routes. This is because, given the importance of KCOM's GC3.1(c) obligations, it needed to be satisfied that the routes being provided were sufficiently diverse to avoid any potential single point of failure. As we have found, KCOM had other options available to it and therefore did not have to utilise the secondary routes proposed by BT.
- 5.73 KCOM has argued that the steps we highlight in paragraph 5.68 are specific in the sense of *"identifying steps that KCOM might have taken with respect to the specific network links that failed, rather than steps that KCOM might have taken to ensure it had diversity across all elements supporting its emergency call traffic."*¹⁶⁰ We disagree with this. We consider that these constitute steps that any reasonable CP should take when designing, planning and implementing its emergency call routing so as to ensure it had the diversity that was required to maintain uninterrupted access to the emergency services, to the greatest extent possible.
- 5.74 For the reasons set out above, we consider that having decided to use BT routes to take its traffic to the BT Switch Connections, there were steps within KCOM's reasonable control that it should have taken in order to discharge its obligations under GC3.1(c). We consider below whether KCOM did take these steps.

¹⁶⁰ KCOM's Response to the 96A Notification, paragraph 3.43.

Did KCOM take all the steps in its reasonable control to secure resilience?

- 5.75 In its Response to the Notification, KCOM submitted that it did take all of the steps that were in its reasonable control to ensure the diversity of its emergency call routing, including the ones that we have set out above. In summary, it has submitted that:
- 5.75.1 KCOM commissioned services from BT MSL (and in effect BT) via the terms of the Horizon contract (see paragraphs 4.40 to 4.52 above) with the explicit and clear objective of ensuring that KCOM's network and services were resilient and that there was no single point of failure;¹⁶¹
 - 5.75.2 KCOM actively monitored BT MSL's performance of its contractual obligations via the BCMS and related actions (see paragraphs 4.60 to 4.62 above);¹⁶²
 - 5.75.3 In taking these actions, KCOM worked collaboratively with BT, sought assurances about network resilience, pushed for planning information and made enquiries. These were all the measures open to KCOM, given the evidence that BT would have refused to provide 'as built' routing information to KCOM.¹⁶³
- 5.76 KCOM has also contended that BT was also under its own regulatory obligations to ensure that the routes on its own network were sufficiently resilient.
- 5.77 KCOM considers that the fact that its efforts were ultimately unsuccessful does not, by itself, demonstrate a contravention of GC3.1(c).
- 5.78 Having considered KCOM's representations and the evidence it has relied on to support them, we remain of the view that KCOM failed to take all the steps within its reasonable control to ensure the diversity of its emergency call traffic. We set out below our reasons below by considering and commenting on each of KCOM's submissions in turn before setting out our conclusions.

Commissioning services from BT MSL under the Horizon contract

- 5.79 KCOM has argued that the terms of the Horizon contract set out to BT MSL *"in precise and clear terms KCOM's requirement for resilience and diversity, including KCOM's specific requirement that the network carrying KCOM traffic must not have a single point of failure"*.¹⁶⁴ It considers that the terms of the Horizon contract *"specifically called out the critical elements that Ofcom considers KCOM should have focused on"*.¹⁶⁵
- 5.80 In particular, KCOM notes the terms set out in:
- 5.80.1 [REDACTED]

¹⁶¹ KCOM's Response to the 96A Notification, paragraphs 3.10-3.13.

¹⁶² KCOM's Response to the 96A Notification, paragraphs 3.30-3.35.

¹⁶³ KCOM's Response to the 96A Notification, paragraphs 3.21-3.29.

¹⁶⁴ KCOM's Response to the 96A Notification, paragraph 3.12(a).

¹⁶⁵ KCOM's Response to the 96A Notification, paragraph 1.14(a).

5.80.2 [X]

5.80.3 [X]

5.80.4 [X]

- 5.81 Having considered the Horizon contract, including the terms set out above, we make the following points in relation to KCOM's submissions.

Design of routing occurred prior to the Horizon contract

- 5.82 It is important to note that the emergency call routing (including the single point of failure) was already in place when BT MSL took over the management of the KCOM network via the Horizon contract in June 2009. KCOM should therefore have already taken steps to ensure the diversity of its emergency call routing at the time it signed the Horizon contract. At this point, the design of the emergency call routing, including the use of the BT ingress routes, had already been decided.
- 5.83 KCOM has not been able to identify any documentary evidence of how these routes were agreed with BT at the outset and it appears to us that had KCOM fully articulated to BT the requirements that the routes have no interdependency with York and had its engineers worked collaboratively with BT's engineers to identify suitable routes, that it is unlikely that they would have ended up with the routes that they did. On the basis of the physical routing alone, the fact that [X most] of the [X]back-up circuits went to or through the exchange that KCOM was seeking to obtain diversity from should have indicated that alternative routing was required. When the signalling was taken into consideration as well, all the routes were dependent on York.
- 5.84 KCOM has said that *"the question of whether the routes were designed correctly in 2007 (or 2009)...is outside the scope of Ofcom's investigation, which is whether KCOM failed to take steps during the Relevant Period that might constitute a contravention of GC3.1(c)."*¹⁶⁶
- 5.85 In respect of this, as set out at paragraph 5.25, KCOM has an ongoing obligation under GC3.1(c) to ensure routing diversity for emergency call services and an omission, that took place before our jurisdiction under sections 96A-96C of the Act took effect on 26 May 2011, may be relevant to whether or not KCOM was able to ensure that diversity during the Relevant Period. Accordingly, we considered the steps that KCOM could have taken at the stage of designing its routing in order to

¹⁶⁶ KCOM's Response to the 96A Notification, paragraph 3.20.

determine whether it would have been technically possible, and within its reasonable control, to ensure diversity during the Relevant Period. We nonetheless make no findings as to whether KCOM contravened its obligations under GC3.1(c) during that earlier period.

BT MSL acted as KCOM's agent

- 5.86 KCOM has contended that BT MSL had functions under the Horizon contract which were relevant to the fulfilment of KCOM's obligations under GC3.1(c). These included functions in relation to: maintaining the network; business continuity planning; network security; disaster recovery; and regulatory compliance, including procuring assistance and information from BT Wholesale [§<]¹⁶⁷ However, KCOM has also submitted that BT MSL's performance of its functions, specifically in relation to business continuity planning and disaster recovery planning, was not "good enough".¹⁶⁸ In KCOM's view, this meant that *"its customers were exposed to risk as a result of that lack of performance"*.¹⁶⁹
- 5.87 At paragraphs 5.90 to 5.95 below, we make certain observations about the terms of the Horizon contract and KCOM's submissions that they made clear KCOM's objectives and specifications in relation to the resilience of its emergency call routing to BT MSL. However, for the purposes of this confirmation decision, it is not necessary to make any findings about whether the Horizon contract was effective in conferring on BT MSL contractual responsibilities for KCOM's emergency call traffic or, if it did, whether BT MSL failed to fulfil them.
- 5.88 This is because the Horizon contract is an outsourcing arrangement, under which BT MSL is contracted to carry out the relevant functions "on KCOM's behalf".¹⁷⁰ In carrying out its functions, it was therefore acting as KCOM's agent and any failing on its part is to be attributed to KCOM for the purpose of determining liability under GC3.1(c).¹⁷¹
- 5.89 On KCOM's own case, KCOM failed to secure its "core objective" – a "robust system for identifying, creating and testing, business continuity and disaster recovery plans for both KCOM's core networks and the key business processes that BT MSL carried out on KCOM's behalf".¹⁷² For these purposes, it is irrelevant whether that failure resulted from shortcomings in BT MSL's performance of its contractual obligations or inaction by KCOM itself. In either case, KCOM, as the CP providing emergency call services to its customers, is responsible for a failure to carry out the necessary steps to maintain uninterrupted access to these services.

¹⁶⁷ [§<]

¹⁶⁸ KCOM's Response to the 96A Notification, paragraphs 2.66 to 2.72.

¹⁶⁹ KCOM's Response to the 96A Notification, paragraph 2.72(d).

¹⁷⁰ KCOM's Response to the 96A Notification, paragraph 2.6.

¹⁷¹ See section 32(4) of the Act which provides that where a person is employed to provide the network or services under the direction or control of another, it is the latter which is treated as the person providing the network or service in question.

¹⁷² KCOM's Response to the 96A Notification, paragraph 2.72 (c).

Observations on the scope of the Horizon contract and the parties' responsibilities

- 5.90 In view of the finding at paragraph 5.88 above, it is not necessary to make any finding as to whether the Horizon contract was effective in conferring responsibility for maintaining access to KCOM's emergency call services on BT MSL, as KCOM has submitted. Nonetheless, we make the following observations about the terms of the agreement.
- 5.91 KCOM itself notes that the Horizon contract is "*much broader than the wholesale supply agreements by which KCOM purchases specific network elements*" (such as the SIA). Under the Horizon contract "*KCOM outsourced a major part of its network operations to BT MSL, [redacted]*".⁷³ The Horizon contract is therefore indicative of a very broad programme undertaken between KCOM and BT MSL both geographically (national in scope), commercially (it affected a broad range of products and services) and technically (network transformation to new technology was a central element).
- 5.92 [redacted]¹⁷⁴ [redacted]
- 5.93 [redacted]
- 5.94 [redacted]
- 5.94.1 [redacted]¹⁷⁵
- 5.94.2 [redacted]¹⁷⁶

¹⁷³ [redacted]

¹⁷⁴ [redacted]

¹⁷⁵ [redacted].

5.94.3 [REDACTED]¹⁷⁷

5.94.4 [REDACTED].¹⁷⁸ [REDACTED]¹⁷⁹

- 5.95 In light of these provisions, it is not clear from the terms of the Horizon contract that we hold that it extends to the BT routes between [REDACTED BT Location 1/BT Location 2] and the BT Switch Connections at York, Leeds and Sheffield. If it does, it is not clear that BT MSL had specific obligations in relation these routes and the emergency call traffic that they were intended to carry. We also query, in light of the terms highlighted above, that KCOM's submissions accurately reflect the delineation of responsibilities between the parties under the agreement in relation to the maintenance of emergency calls services.

Steps taken by KCOM to monitor BT MSL's performance

- 5.96 As set out in Section 4, KCOM has provided evidence of actions that it took to ensure that BT MSL performed its obligations under the Horizon contract. It argues that:

- 5.96.1 Correspondence early in the Relevant Period (2011) *"shows that KCOM at that time placed a priority specifically on the restoration of 'emergency services' ahead of all other restoration priorities in the event of a disaster"*,¹⁸⁰
- 5.96.2 The BCMS process in 2012 *"makes it clear that KCOM not only actively monitored progress towards the objectives set out in the Horizon Agreement, it acted to push for better outcomes when it became clear that BT's performance was inadequate"*,¹⁸¹ and
- 5.96.3 KCOM's actions *"subsequent to the Horizon Agreement and during the Relevant Period show that KCOM continued to communicate that priority to BT"*.¹⁸²

- 5.97 We acknowledge that KCOM took steps during the Relevant Period to monitor BT MSL's performance of its contractual obligations.

¹⁷⁶ [REDACTED]

¹⁷⁷ [REDACTED]

¹⁷⁸ [REDACTED]

¹⁷⁹ [REDACTED]

¹⁸⁰ KCOM's Response to the 96A Notification, paragraph 3.12(b).

¹⁸¹ KCOM's Response to the 96A Notification, paragraph 3.12(c).

¹⁸² KCOM's Response to the 96A Notification, paragraph 3.12(d).

- 5.98 However, the actions that KCOM has highlighted relate to a general programme to design and implement business continuity and disaster recovery plans, which included examination of BT MSL's performance of its contractual obligations. We have not seen evidence of specific consideration of KCOM's emergency call services or routing in any subsequent risk assessment under this general programme.
- 5.99 In fact, the evidence indicates that whilst 15 risk assessments were completed on the KCOM network as a result of KCOM's interventions, none of these examined the BT routes that KCOM was using for the conveyance of emergency call traffic.¹⁸³ From the information supplied by KCOM, one of the risk assessments¹⁸⁴ examined the telephony network as well as the underlying SDH 'ring' networks (both national and Hull-specific), and recognised that these assets were 'Critical'. However, the transmission paths on which emergency call traffic between these networks were conveyed between these regional and national rings were not included in this risk assessment.

KCOM has carried out all the steps identified by Ofcom which were possible

- 5.100 KCOM also submitted that:

"All but one of the things that Ofcom considers that KCOM could have done, KCOM did in fact do, through the Horizon Agreement or its subsequent efforts to drive better performance from BT. (The exception is to obtain 'as-built' information – BT's own evidence to Ofcom suggests that this information would not have been provided to KCOM under any circumstances)."

- 5.101 For the reasons set out below, we remain of the view that KCOM did not take all the steps within its reasonable control to secure resilience for its emergency call services.

Collaborative working with BT

- 5.102 As set out at paragraphs 5.83 above, we consider that the configuration of the primary and back up routes for KCOM's emergency call traffic, incorporating a single point of failure at York, suggests that there was a lack of collaboration between KCOM and BT's engineers when the routes were initially selected in 2009.
- 5.103 We acknowledge the Horizon contract and the steps taken as part of KCOM's BCMS project provide evidence of collaboration between KCOM and BT MSL. However, as noted, there is a lack of specificity in both the Horizon contract and the BCMS risk assessments about their application to emergency call traffic. Accordingly, we are not satisfied they are sufficient to demonstrate that this collaboration extended, or was carried out effectively, in relation to securing resilience for KCOM's emergency call services.

¹⁸³ As set out at paragraph 4.59, KCOM did not identify these risk assessments as relating to the routing or conveyance of emergency call traffic in its First Response. It described them as "low level" risk assessments which it provided for "completeness".

¹⁸⁴ Information derived from the Service Platform Mapping Report (available at Annex 29) which was embedded in a BCMS closure document entitled "Work Stream 5 Closure Document – Initiation of BCMS (carry out 1st cycle) and Lessons Learnt Statement" (available at annex 30).

- 5.104 To the extent that KCOM was relying on BT MSL to liaise with BT Wholesale for these purposes, we attribute any failure by BT MSL in this regard to KCOM, on the grounds that BT MSL acts as KCOM's agent for the purposes of the Horizon contract.¹⁸⁵

KCOM sought assurances concerning network resilience

- 5.105 KCOM cites specific terms of the Horizon contract to show that it sought assurances about network resilience on a periodic and ongoing basis.¹⁸⁶ However, as explained above, it is not clear from the face of the Horizon contract that it extends to the BT routes between [X BT Location 1/BT Location 2] and the BT Switch Connections at York, Leeds and Sheffield. Similarly, it is not apparent that the risk assessments carried out as part of the BCMS project (on which KCOM also relies) specifically examined network resilience for emergency call traffic.

- 5.106 To the extent that KCOM was relying on BT MSL to liaise with BT Wholesale for these purposes, our finding at paragraph 5.104 also applies in this context.

KCOM took steps to obtain better planning information from BT and made enquiries

- 5.107 KCOM has submitted that the Horizon contract and the BCMS project show that it sought information from BT about the resilience of its network. In relation to these submissions, we refer to our responses at paragraphs 5.102 – 5.103 above.
- 5.108 KCOM has further submitted that it took action as result of issues that it identified with BT MSL's performance, specifically that it sought to tightly manage BT (as through the BCMS process) and, where necessary, to bring some BCP functions in-house. We observe however, that there is no evidence of specific action that KCOM took in relation to the routing of its emergency call traffic. Accordingly, it is not apparent that KCOM's enquiries related specifically to these issues, even though it had specific and onerous obligations in relation to this traffic and had made particular arrangements for its conveyance for hand over to BT.
- 5.109 To the extent that KCOM was relying on BT MSL to liaise with BT Wholesale for these purposes, our finding at paragraph 5.104 also applies in this context.

No access to in-built routing information

- 5.110 In relation to KCOM's submission in relation to 'as-built' information not being provided by BT, we refer to our finding at paragraph 5.72 above that had KCOM found itself in a position where BT could not (or was unwilling to) provide it with sufficient information or assurances about the diversity of its routing, we consider this should have prompted KCOM to reconsider its decision to use BT's routes.

BT's performance of its regulatory obligations

- 5.111 In KCOM's First Written Response and its Response to the Notification, KCOM submits that BT was under obligations of its own under GC3.1(c) in relation to the routes that failed and says that:

¹⁸⁵ See KCOM's Response to the 96A Notification, paragraphs 2.10 and 2.11 as well as paragraph 3.26. KCOM does not make this point explicitly in its submissions and we make no finding as to whether BT MSL had such an obligation under the Horizon contract.

¹⁸⁶ KCOM's Response to the 96A Notification, paragraph 3.25.

“As a matter of fact, the ‘measures’ adopted by KCOM for the purposes of its compliance with GC3.1(c) included, in effect, to rely on BT’s performance of those obligations.”¹⁸⁷

- 5.112 We do not consider that BT’s regulatory responsibilities are relevant to the assessment of whether KCOM has breached GC3.1(c).
- 5.113 As we have set out above, the relevant consideration is whether KCOM did everything it could have done to ensure that its emergency call routing was sufficiently diverse. It is not sufficient for KCOM to have assumed that BT was under its own regulatory obligations in relation to these specific routes that KCOM was utilising to take its traffic to the relevant BT Switch Connections. As set out at paragraphs 5.66 to 5.74, KCOM could, and should, have taken further steps to ensure that the routes it was utilising were fit for its own purpose, and its own regulatory responsibilities.

Hindsight bias and “best efforts failing”

- 5.114 Finally, KCOM has argued that its “best efforts failing” does not mean a contravention of GC3.1(c) has arisen. It claims that *“hindsight bias appears, unconsciously, to have clouded Ofcom’s reasoning in the Notification”*.¹⁸⁸ It also argues that Ofcom’s thinking may be skewed by the assumption that KCOM could “always have done more” to avoid the incident.¹⁸⁹
- 5.115 We disagree with KCOM. As set out at paragraph 5.73, we consider that the steps we have highlighted in paragraph 5.68 are reasonably identifiable as appropriate and achievable and that KCOM (or someone acting on KCOM’s behalf) could, and should, have taken when designing, planning and implementing its emergency call routing so as to ensure it had the diversity that was required to maintain uninterrupted access to the emergency services, to the greatest extent possible. Accordingly, we consider that KCOM’s failure to take these, or other similar steps, does amount to a breach of GC3.1(c) and the requirement to take all possible steps to ensure the diversity of its emergency call routing.

Conclusions

- 5.116 Given all of the above, we are not satisfied that the actions that KCOM took in setting the terms of the Horizon contract, and in monitoring BT MSL’s performance of its contractual obligations were sufficient to demonstrate that KCOM took all of the steps in its reasonable control to ensure the diversity of its emergency call routing.
- 5.117 In summary, we say this because:
- 5.117.1 The call routing, including the single point of failure, was put in place prior to the Horizon contract coming into force. KCOM should therefore have already taken the steps (or similar) we have set out at paragraph 5.68 above, and there is insufficient evidence that it did so when the routing was set up;

¹⁸⁷ KCOM’s First Written Response, paragraph 3.17.

¹⁸⁸ KCOM’s First Written Response, paragraph 1.12. See Also KCOM’s First Written Response, Section 6. In KCOM’s Response to the 96A Notification it notes at paragraph 3.42 that it *“affirms but does not repeat the points it has made previously about hindsight bias”*.

¹⁸⁹ KCOM’s Response to the 96A Notification, paragraphs 3.42 to 3.44.

- 5.117.2 The Horizon contract is an outsourcing arrangement and therefore on KCOM's own case that BT MSL's performance of its obligations under the contract was not "good enough", KCOM is responsible for the alleged omissions of its agent;
- 5.117.3 The Horizon contract is broad in scope and the terms of the contract are similarly broad. Whilst there are general terms relating to the diversity of KCOM's network, there is no specific mention of KCOM's emergency call routing or traffic. Therefore we do not consider that the Horizon agreement sets out in clear terms that its scope extends to the BT routes between [X BT Location 1/BT Location 2] and the BT Switch Connections at York, Leeds and Sheffield nor (assuming it does) that BT MSL has specific obligations in respect of them and resilience of KCOM's emergency call traffic that they were intended to carry;
- 5.117.4 whilst the actions that KCOM has highlighted are indicative that KCOM monitored BT MSL's performance of its contractual obligations, there is no evidence of specific consideration of KCOM's emergency call services or routing in risk assessments that were carried out; and
- 5.117.5 KCOM retained both responsibilities and capabilities to audit, review and assess network architectures and associated routing.
- 5.118 In addition, whilst we have considered KCOM's submissions regarding BT's regulatory responsibilities under GC3.1, we do not consider these are relevant to our assessment of KCOM's compliance with GC3.1(c).

Conclusions on a breach of GC3.1(c)

- 5.119 Having taken account of the representations made to us by KCOM and for the reasons set out above, we are satisfied that KCOM failed to take all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations in that:
- 5.119.1 it failed to ensure it had diverse and resilient routing in place for its emergency call traffic during the Relevant Period; and
- 5.119.2 it would have been technically feasible and within KCOM's reasonable control to have taken steps to have secured diverse and resilient routing for its emergency call traffic; and
- 5.119.3 it failed to take steps to exercise oversight of, or seek assurances in relation to, the diversity and resilience of the secondary routes for its emergency call traffic.
- 5.120 Given this, we are satisfied that KCOM has contravened GC3.1(c) during the Relevant Period.

Section 6

Penalty

Summary

- 6.1 Ofcom's decision is that that we should impose a penalty of £900,000 on KCOM for its contravention of GC3.1(c).
- 6.2 Our decision aims to incentivise CPs to comply with their regulatory obligations and is guided by our principal duty of furthering the interests 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 KCOM failed to ensure sufficient resilience in its emergency call routing during the Relevant Period, which is a long and sustained period, and that this failure was in breach of GC3.1(c).
- 6.4 Although it appears that KCOM had taken steps to build resilience into its emergency call routing, it became clear following the Incident that the routing of KCOM's emergency call traffic had a single point of failure at the BT York Stonebow exchange. We consider that KCOM failed to take sufficient steps to enable it to ensure that it had diverse and resilient routing in place for its emergency call traffic despite the fact it would have been technically feasible and within KCOM's reasonable control to have done so.
- 6.5 We have taken account of the actual harm which KCOM caused to its end-users as a result of the contravention. When the York Stonebow exchange flooded, KCOM's entire customer base on the Hull network were unable to contact the emergency organisations on 999 and 112 for a period of almost four hours on the night of 27/28 December 2015.
- 6.6 In mitigation, we have taken account of the fact that the breach of GC3.1(c) does not appear to have been deliberate or reckless and that KCOM appears to have made an effort to secure diversity (even if we ultimately conclude that it failed to do so). KCOM has also cooperated fully with us throughout the investigation.
- 6.7 Our assessment also takes account of the steps that KCOM took following the Incident to ensure that its emergency call routing was sufficiently diverse and resilient.
- 6.8 Our view is that the conduct warrants the imposition of a penalty:
 - to reflect the seriousness and duration of the infringement;
 - to reflect the degree of actual and potential harm caused by KCOM's contravention;
 - which takes into account that KCOM is a communications provider that serves thousands of customers with an annual turnover of hundreds of millions of pounds; and

- which is sufficiently substantial to incentivise compliance with regulatory obligations by KCOM and other CPs in future; but
- which reflects our view that the contravention did not occur deliberately or recklessly and which reflects KCOM's attempts to route its emergency calls in a diverse manner; and
- acknowledges KCOM's cooperation throughout the investigation.

6.9 Accordingly, and as set out more fully below, we have imposed on KCOM a penalty of £900,000. Our view is that this would be appropriate and proportionate to the contravention in respect of which it is imposed, and will incentivise both KCOM, and the wider industry, to ensure they are complying with GC3.1 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 its 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 KCOM does not appear to have acted deliberately or recklessly, the Incident exposed the single point of failure in its emergency call routing, which put the ability of its customers to call the emergency organisations at risk for a period of four and a half years, and had the potential to cause significant harm to public health and security during that period. This is in addition to the actual harm caused to KCOM's customers when its emergency call services failed on the night of the Incident.

6.13 In light of the individual circumstances of this case, we consider a financial penalty is appropriate and a proportionate response to the nature and seriousness of KCOM's contraventions. 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

6.14 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

6.15 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 96B¹⁹⁰ and must specify a period within which the person notified may make representations in response.

- 6.16 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.
- 6.17 Sections 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.
- 6.18 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.
- 6.19 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 2015.¹⁹¹

The Penalty Guidelines and relevant factors

- 6.20 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.¹⁹² 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;
 - 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 KCOM's contraventions and its size and turnover;
 - c) the following factors 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 of KCOM's contravention;
 - ii) the degree of harm, whether actual or potential, caused by that contravention;

¹⁹⁰ Section 96A(2)(e) of the Act.

¹⁹¹ "Ofcom Penalty Guidelines. S.392 Communications Act 2003", Guidelines, 3 December 2015. Available at http://www.ofcom.org.uk/content/about/policies-guidelines/penalty/Penalty_guidelines_2015.pdf.

¹⁹² Penalty Guidelines, paragraph 11.

- iii) the duration of KCOM's contravention;
- iv) any gain (financial or otherwise) made by KCOM as a result of the contravention;
- v) whether in all the circumstances, KCOM took appropriate steps to prevent the contravention;
- vi) 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;
- vii) whether the contravention continued, or timely and effective steps were taken to end it, once KCOM became aware of it;
- viii) any steps KCOM has taken for remedying the consequences of the contravention;
- ix) whether KCOM has a history of similar contraventions; and
- x) the extent to which KCOM has cooperated with our investigation.

6.21 In addition, the Penalty Guidelines set out that:

"Ofcom will have regard to any relevant precedents set by previous cases, but may depart from them depending on the facts and the context of each case. We will not, however, regard the amounts of previously imposed penalties as placing upper thresholds on the amount of any penalty."

6.22 We therefore also consider relevant precedents in making our decision on the appropriate and proportionate amount of any penalty.

Seriousness

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 the emergency organisations by calling 999 or 112 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 liable to regard any contravention of this General Condition as inherently serious, because it carries a significant risk of substantial harm to citizens and consumers.

Degree of harm

6.25 As discussed above, any breach of GC3.1(c) has by its very nature the risk of causing harm to citizens and consumers as it puts at risk their ability to contact the emergency organisations. In addition to this potential harm, we have considered the actual harm caused to KCOM's end-users by the outage of the 999 service on the night of 27/28 December and having done so, we consider this contributes to the seriousness of the contravention.

- 6.26 When the BT York Stonebow exchange was lost as a result of flooding, KCOM's customers in the Hull area (around 187,000 lines) were unable to access emergency organisations by dialling 999 or 112 for a period of three and three-quarter hours. The outage was of material duration and significantly increased the risk of substantial harm to citizens and consumers.
- 6.27 During the period of outage, 74 calls were attempted to emergency organisations from 34 different numbers. Each call was made by an individual or an alarm system trying to contact the emergency organisations to report an event in which public health or safety was considered to be at risk.
- 6.28 We have no evidence that the resulting delays in contacting the emergency organisations contributed to any physical harm suffered by an individual during this period, although there was a serious risk that this could have occurred.¹⁹³ We consider it highly likely, however, that the failure of KCOM's emergency call service would have caused emotional distress to the individuals who were unable to reach the emergency organisations by calling 999 or 112 and others who witnessed this. Calls to 999 and 112 invariably occur in highly stressful situations and the ability to speak to a trained call handling agent who can provide advice and route their call through to the appropriate emergency organisation can provide reassurance or relief. By comparison, having a 999/112 call fail is likely to increase the anxiety felt by the caller and others at the scene. We consider that the call log provided by KCOM showing a number of repeat calls to 999 while the service was unavailable provides evidence of behaviour consistent with increasing anxiety on the part of callers.
- 6.29 We consider the fact that KCOM's breach resulted in the actual failure of provision of access to the emergency organisations, and the actual harm that arose as a consequence, to be a factor that we should take into consideration when assessing the seriousness of KCOM's breach of GC3.1(c). Although the speed with which access to the emergency organisations was restored once the outage was identified counts in KCOM's favour, this is counteracted by the fact that it took nearly two hours for the outage to be identified.

Duration

- 6.30 For the reasons set out in Section 5, we consider that for the Relevant Period KCOM did not have in place the necessary measures (i.e. diverse and resilient emergency call routing) to ensure uninterrupted access to the emergency organisations.
- 6.31 We therefore consider KCOM were in breach of GC3.1(c) from 26 May 2011 to 28 December 2015, on an ongoing basis, as the single point of failure existed throughout this period and KCOM failed to take measures that might have identified it. This is a prolonged and sustained period and is a factor that we have taken into consideration in proposing the level of penalty that we consider appropriate.

¹⁹³ 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: http://www.london-fire.gov.uk/Documents/London_Fire_Brigade_Fire_Facts_Incident_response_times_2013.pdf. [X]

- 6.32 During this period KCOM's emergency call service was vulnerable and at unnecessary risk of a service failure due to the fact that all of its emergency call traffic was dependant on the BT York Stonebow exchange.

Any gain (financial or otherwise) made by KCOM

- 6.33 We have also considered whether KCOM made any gain (financial or otherwise) as a result of the contravention. We note that it is almost always the case that failure to comply with regulation is cheaper than compliance. In this case, however, we consider that the costs of compliance that were avoided over the period of the contravention would not have been significant and therefore we do not consider it necessary to quantify this cost precisely.

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

- 6.34 There is no evidence that KCOM deliberately or recklessly contravened its obligations under GC3.1(c). Indeed, KCOM appears to have (i) taken steps to ensure diversity on its own network by consolidating emergency calls at two separate (but linked) exchanges in Hull, and (ii) sought to ensure that the routing of the emergency calls to the BT Switch Connections was diverse by putting in place back-up routes to three separate BT Switch Connections.
- 6.35 For the reasons discussed in Section 5, we consider that KCOM was responsible for the emergency calls up to the point of interconnect with BT and that there were steps that it could have taken, but didn't, that might have given it the opportunity to identify that a single point of failure existed. We recognise, however, that once the routes were put in place then the opportunities to identify the single point of failure were more limited – though not non-existent – and that this is a relevant factor to take into consideration when setting the penalty.
- 6.36 KCOM has provided evidence of how it sought to ensure the overall diversity and resilience of its network by entering into, and maintaining oversight of, the Horizon contract. It has contended that the steps it took in this regard and the division of responsibilities under the contract should be taken into account in the assessment of penalty.
- 6.37 We have taken account of the evidence KCOM provided in relation to its monitoring of the Horizon contract in assessing the level of penalty, as we consider it does indicate that KCOM sought to ensure the diversity of its network and call routing in general when it handed responsibilities over to BT MSL for the operation and management of its network under the Horizon contract.
- 6.38 While terms of the Horizon contract demonstrate that KCOM was cognisant of the need to secure a robust network and took steps to achieve that, as set out at paragraphs 5.75 to 5.115, it is not clear that these were clearly directed at KCOM's emergency call services or the BT back up routes between [X BT Location 1/BT Location 2] and York, Leeds and Sheffield which contributed to the single point of failure in this case. For the reasons given, we are not persuaded that by entering into the Horizon contract, and the action it took subsequently to monitor BT MSL's performance, KCOM took all necessary steps within its reasonable control to secure resilience of the routing for its emergency call services.
- 6.39 Accordingly, while we do not consider that the contravention in this case resulted from deliberate or reckless actions on the part of KCOM, we are satisfied that it is

sufficiently culpable for the omissions which led to the failure of its emergency calls services to justify a penalty.

Steps taken to end the contravention and to remedy the consequences

- 6.40 We consider that whilst appropriate steps were taken by KCOM (or on its behalf) to bring an end to the contravention, there was a delay in KCOM realising that its emergency call services had failed.
- 6.41 In particular, the Government issued a warning to CPs that the BT York Stonebow exchange was flooding and this this could affect their communications services at 21:43 on the 27 December 2015.¹⁹⁴ Call records show that the first emergency call failed at 21:58 on 27 December 2015.¹⁹⁵ However, it appears that it was not for another hour that KCOM's agent, BT MSL, logged the incident¹⁹⁶ and it was then a further hour before BT MSL discovered that KCOM's emergency call traffic had failed. Even then it was a call from Humberside Police noting that emergency calls did not appear to be coming through that raised the alarm, rather than monitoring by KCOM or BT MSL of the emergency call traffic.¹⁹⁷
- 6.42 Once the outage was identified, BT MSL acted swiftly to restore the service, putting in place alternative routing for the emergency call traffic around two hours after first becoming aware that the service had failed so that KCOM's customers were able to make 999 calls from 01:43 on 28 December 2015.
- 6.43 We note that KCOM has subsequently undertaken to carry out regular risk assessments in relation to its provision of calls to the emergency organisations. We also note the action that has been taken to improve the monitoring of KCOM's emergency call traffic and highlight any loss of service that may arise in the future.¹⁹⁸

History of contraventions and co-operation

- 6.44 Ofcom has not previously issued a notification to KCOM under section 96A of the Act for a contravention of GC3.1 or any of the other General Conditions.
- 6.45 This investigation was triggered by KCOM's notification to us of the Incident, in accordance with KCOM's obligations under section 105B of the Act. Since the Incident, KCOM has provided us with information in a timely manner and has co-operated fully with our investigation.

Incentivising compliance

- 6.46 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

¹⁹⁴ See paragraph 4.71 above.

¹⁹⁵ The Report, Annex 2, page 12.

¹⁹⁶ The RCA, attachment to paragraph 5.4 titled "27th December 2015 Time line", pages 2 and 3.

¹⁹⁷ See paragraph 4.72 above.

¹⁹⁸ See paragraphs 4.75 to 4.82 above.

*and turnover of the regulated body when considering the deterrent effect of any penalty.*¹⁹⁹

- 6.47 In this respect, as noted above, it appears that KCOM did not intend to breach its regulatory obligations and that it made an effort to secure diversity (even if we ultimately conclude that it failed to do so). We also note that it is likely that the costs of compliance that were avoided over the period of the contravention would not have been significant.
- 6.48 However, we consider that KCOM failed to take sufficient steps to ensure that its emergency call routing was diverse and resilient, 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 on the one hand, but that is also at a level that will incentivise KCOM, and the wider industry, to ensure that they comply with the requirements of GC3.1(c) at present, and on an ongoing basis.
- 6.49 As noted above, the statutory maximum penalty Ofcom may impose on KCOM is ten per cent of its turnover for its relevant business for the period 1 April 2016 to 31 March 2017.²⁰⁰ KCOM's results for the financial year ended 31 March 2017 indicate that KCOM's turnover for 2016/17 was £331.3 million.²⁰¹ The maximum penalty Ofcom could impose on it would therefore be £33.1 million. Given this, we consider a substantial penalty is required to achieve our aim of having an impact on it that incentivises compliance in future (as well as signalling to other CPs that non-compliance by them may result in penalties having a similar impact).
- 6.50 We note that KCOM's breach of its obligations under GC3.1(c) relates to its Hull and East Yorkshire (HEY) business division. KCOM submitted that Ofcom should only have regard to the turnover for that division in calculating the maximum amount of penalty that can be imposed. In this respect, we note that according to section 97(5) of the Act, "relevant business" means in this context "*so much of any business carried on by the person that consists in any one or more of the following: a) the provision of an electronic communications network...*". The Act therefore requires Ofcom to have regard to the regulated body's total turnover related to the provision of electronic communications services as the appropriate reference point for assessing the penalty amount, rather than considering the particular part of the business that is responsible for the breach. We therefore consider the relevant reference point to be KCOM's total turnover of £331.3 million.

Relevant precedents

- 6.51 Ofcom recently concluded an investigation into Three in relation to its compliance with GC3.1(c), where we identified that there was a single point of failure in Three's network and concluded that as a consequence it had failed to take all necessary measures to maintain access to emergency organisations.²⁰² In that case we imposed a penalty of £1.89 million on Three, though the calculation for this figure

¹⁹⁹ Penalty Guidelines, paragraph 11.

²⁰⁰ Given that this Confirmation Decision is issued prior to April 2018, this is the relevant period for the purposes of calculating the maximum penalty, as defined in section 97(5) of the Act.

²⁰¹ KCOM Group PLC - Annual report and accounts 2016/17:

<http://www.kcomplc.com/media/1625/annual-report-2016-17.pdf>

²⁰² See: https://www.ofcom.org.uk/about-ofcom/latest/bulletins/competition-bulletins/all-closed-cases/cw_01190

included a 30% discount to reflect Three accepting liability and entering into a voluntary settlement with Ofcom.

- 6.52 Given that the Three investigation considered the same General Condition that is under review in this investigation and that the nature of the breach was similar, we have therefore had due regard to the level of penalty imposed on Three when setting the level of penalty in this case.
- 6.53 KCOM has argued that differences between facts in the two cases suggest that Ofcom should reduce the level of penalty that it imposes on KCOM.²⁰³ In particular, KCOM notes that:
- 6.53.1 The number of customers affected by the outage in the Three case appeared significantly larger than the number affected by KCOM's outage;
 - 6.53.2 The single point of failure in the Three case was not the result of an event within another operator's network but rather Three's own network, which it could observe and detect directly;
 - 6.53.3 There is nothing to suggest that KCOM's failure to maintain access to the emergency organisations was more serious than Three's, suggesting that the penalties for each operator should be proportionate to their scale and operations; and
 - 6.53.4 As a proportion of revenue, the penalty proposed for KCOM is more severe than that imposed on Three, noting that KCOM's revenue is around six times smaller than Three's.
- 6.54 We have considered the points that KCOM has made but disagree with its conclusions. In particular, we disagree with KCOM's assertion that its contravention of GC3.1(c) was no more serious than that of Three:
- 6.54.1 Although there was a single point of failure in the networks of both KCOM and Three, the single point of failure in Three's emergency call routing did not cause the incident that led to the loss of Three's emergency call service. This contrasts with KCOM's contravention, where the single point of failure was the direct cause of the loss of access to the emergency organisations.
 - 6.54.2 Whilst there was significant potential for harm resulting from the Three contravention, there was no actual harm caused to its end-users as the single point of failure did not cause loss of access to the emergency organisations. By contrast, KCOM's customers suffered actual harm as they were unable to access the emergency organisations for a period of nearly four hours.
- 6.55 The fact that the single point of failure in KCOM's emergency call routing caused the loss of access to the emergency organisations and that this led to actual harm to consumers means that we consider KCOM's contravention of GC3.1(c) to be more serious than Three's breach of this condition. Therefore, although we have taken into consideration the comparative differences in the number of customers potentially affected and the degree of visibility of the network, we have concluded that the more

²⁰³ KCOM's Response to the 96A Notification, paragraph 4.8.

serious nature of the breach means that it is appropriate to impose a proportionately higher level of penalty on KCOM than that which we imposed on Three.

Ofcom's conclusions on the level of penalty

- 6.56 Considering all of the above factors in the round, the penalty we have decided to impose on KCOM is £900,000.
- 6.57 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 serious nature of KCOM's contravention of GC3.1; and
 - to incentivise KCOM and other CPs to ensure they are complying with their regulatory obligations, particularly GC3.1(c), at present and on an ongoing basis.
- 6.58 Ofcom considers that a penalty of the proposed 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 KCOM's cooperation and the fact that KCOM 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.

Conclusions

- 6.59 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 KCOM.

Section 7

Conclusions and action required by KCOM

Contravention of GC3.1

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

Steps that should be taken by KCOM

- 7.2 As part of ensuring it takes all necessary measures to maintain, to the greatest extent possible, uninterrupted access to the emergency organisations as part of its publicly available telephone services, KCOM is required to take the following steps, to the extent it has not already taken them:
- i) 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 the BT York Stonebow exchange; and
 - ii) 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) being issued, KCOM should provide Ofcom with a description of the processes it has in place for the ongoing review and management of the risks associated with the conveyance of its emergency call traffic.

Proposed Penalty

- 7.4 For the reasons set out in this document, Ofcom is minded to impose a penalty of £900,000 on KCOM in respect of its contravention of GC3.1(c).

List of Annexes

Annex 1	[X]
Annex 2	[X]
Annex 3	[X]
Annex 4	[X]
Annex 5	[X]
Annex 6	[X]
Annex 7	[X]
Annex 8	[X]
Annex 9	[X]
Annex 10	[X]
Annex 11	[X]
Annex 12	[X]
Annex 13	[X]
Annex 14	[X]
Annex 15	[X]
Annex 16	[X]

Annex 17	[✗]
Annex 18	[✗]
Annex 19	[✗]
Annex 20	[✗]
Annex 21	[✗]
Annex 22	[✗]
Annex 23	[✗]
Annex 24	[✗]
Annex 25	[✗]
Annex 26	[✗]
Annex 27	[✗]
Annex 28	[✗]
Annex 29	[✗]
Annex 30	[✗]

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,²⁰⁴ 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

²⁰⁴ 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.

notification in accordance with section 48(1) of the Act entitled ‘*Notification setting general conditions under section 45 of the Communications Act 2003*’.²⁰⁵ 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 2003.²⁰⁶

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 GC3.1²⁰⁷ 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 KCOM Group PLC (KCOM), whose registered company number is 2150618. KCOM’s registered office is 37 Carr Lane, Hull, East Yorkshire, HU1 3RE.

Notification given by Ofcom under 96A

A1.9 On 2 June 2017, Ofcom gave KCOM a notification under section 96A of the Act as Ofcom had reasonable grounds for believing that KCOM had contravened GC3.1(c). Specifically, that between 26 May 2011 and 28 December 2015, KCOM failed to take all necessary measures to maintain to the greatest extent possible uninterrupted access to the emergency organisations as part of its publicly available telephony service.

²⁰⁵ Available at:

http://www.ofcom.org.uk/static/archive/oftel/publications/eu_directives/2003/cond_final0703.pdf.

²⁰⁶ A consolidated version of the General Conditions is available at:

http://stakeholders.ofcom.org.uk/binaries/telecoms/ga/GENERAL_CONDITIONS_22Sept2014.pdf.

²⁰⁷ 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.

- A1.10 The Section 96A Notification specified the penalty that Ofcom was minded to impose on KCOM in respect of the contravention of General Condition 3.1(c).
- A1.11 The Section 96A Notification also allowed KCOM 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 30 June 2017 KCOM provided written representations to Ofcom on the matters set out.
- A1.13 Having taken account of the representations made to us by KCOM and for the reasons set out in the Explanatory Statement, we are satisfied that KCOM failed to take all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations in the period 26 May 2011 to 28 December 2015 in that:
- 1.13.1 it failed to ensure it had diverse and resilient routing in place for its emergency call traffic during the Relevant Period; and
 - 1.13.2 it would have been technically feasible and within KCOM's reasonable control to have taken steps to have secured diverse and resilient routing for its emergency call traffic; and
 - 1.13.3 it failed to take steps to exercise oversight of, or seek assurances in relation to, the diversity and resilience of the secondary routes for its emergency call traffic.
- A1.14 Accordingly, Ofcom is satisfied that KCOM has contravened GC3.1(c) in the period 26 May 2011 to 28 December 2015. Ofcom has decided to give KCOM 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

- A1.15 As part of ensuring that it takes all necessary measures to maintain, to the greatest extent possible, uninterrupted access to the emergency organisations KCOM is required to take the following steps, to the extent it has not already taken them:
- i) 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 the BT York Stonebow exchange; and
 - ii) 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).

Within one month of any final section 96C Notification being issued, KCOM should provide Ofcom with a description of the processes it has in place for the ongoing review and management of the risks associated with the conveyance of its emergency call traffic.

- A1.16 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.²⁰⁸

Penalty

- A1.17 Ofcom has determined that KCOM must pay a penalty of £900,000 on KCOM in respect of its contravention of GC3.1(c).
- A1.18 KCOM has until 6 September 2017 to pay Ofcom the penalty. If not paid within the period specified it can be recovered by Ofcom accordingly.²⁰⁹

Interpretation

- A1.19 Words or expressions used in this Notification have the same meaning as in the GCs or the Act except as otherwise stated in this Notification.

Selina Chadha



Director of Consumer Policy

as decision maker for Ofcom

8 August 2017

²⁰⁸ Communications Act 2003, section 96C(6).

²⁰⁹ Communications Act 2003, section 96C(7).