Confirmation Decision under section 96C of the Communications Act 2003

Confirmation Decision served on Vonage Limited by the Office of Communications for contravention of General Condition 3.1(c)

Non-confidential version - redactions are indicated with [✂]

Issue date: 11 December 2018

Contents

Section

1. Overview

Introduction

1.1 This document explains Ofcom's decision to issue Vonage Limited (Vonage) with a Confirmation Decision under section 96C of the Communications Act 2003 (the Act) in respect of its contravention of General Condition 3.1(c) of the General Conditions of Entitlement (GC3.1(c)).[1] The Confirmation Decision is at Annex 3.

1.2 GC3.1(c) requires communications providers (CPs) to take all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations as part of any publicly available telephone service that they offer. Further details on the regulatory framework for this investigation can be found at Annex 1.

1.3 Protecting consumers from harm is one of Ofcom's stated goals in the annual plan.[2] Given that access and/ or resilience issues which affect the availability of emergency calls create a real risk to citizens' safety of life, Ofcom will always take particularly seriously any notifications by CPs[3] regarding such issues.

1.4 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.

1.5 In particular, CPs should ensure that their change implementation processes include emergency call testing and that all possible steps are taken to ensure that testing is completed. Further, CPs should ensure their monitoring procedures enable them to maintain sufficient oversight of their network operations and to identify and escalate issues affecting emergency calls access as appropriate.

Finding under GC3.1

1.6 On 25 January 2018, in line with its obligations under section 105B of the Communications Act 2003 (the Act), Vonage notified Ofcom of an incident that affected the availability of its emergency call services from 06.00 on 17 January 2018 to 19.00 on 22 January 2018 (the Incident).

---

[1] Ofcom published revised General Conditions on 19 September 2017 which came into force on 1 October 2018. Since the Incident described in this document occurred prior to 1 October 2018, the relevant investigation was opened under the version of the conditions that applied at that date.
https://www.ofcom.org.uk/__data/assets/pdf_file/0023/106394/Annex-14-Revised-clean-conditions.pdf

[2] See Ofcom's Annual Plan 2018/19, page 9 https://www.ofcom.org.uk/__data/assets/pdf_file/0017/112427/Final-Annual-Plan-2018-19.pdf

[3] Under section 105B of the Communications Act 2003, CPs are required to notify Ofcom of 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.

1.7 On 3 April 2018, Ofcom opened an investigation into whether there had been a contravention of Vonage's obligations under GC3.1 and/ or section 105A of the Act (the Investigation). Details of Ofcom's Investigation and information gathering can be found at Annex 2.

1.8 Having considered the information available to us, including the incident report Vonage submitted to Ofcom on 25 January 2018 (the Incident Report[4]) and the information that we have requested from Vonage, we are satisfied that Vonage contravened GC3.1(c) throughout the duration of the Incident, by failing to take all necessary measures to maintain, to the greatest extent possible, uninterrupted access to the emergency organisations on 999 and 112 as part of the publicly available telephone service that they offered. We say this because:

a) despite the fact Vonage had a policy in place to test emergency calls when completing a significant routing change, it failed to take sufficient steps to ensure that emergency call testing was completed. This failure was particularly serious as it meant that no emergency call testing was completed in relation to the routing change that led to the Incident and ultimately led to Vonage's emergency call service failing; and

b) at the time of the Incident Vonage did not have separate monitoring in place for its emergency call traffic which meant it was unaware that its emergency call service was unavailable for 5.5 days; and

c) it would have been possible and proportionate for Vonage to have taken further steps to ensure that emergency call testing was completed when implementing the change and to have had emergency call monitoring in place for its emergency call service.

1.9 We require Vonage to take all necessary measures to maintain, to the greatest extent possible, access to emergency organisations so as to comply with the requirements of GC3.1(c). Specifically, we now require Vonage to ensure (to the extent it has not already done so) that:

i) its change implementation processes include emergency call testing and that all possible steps are taken to ensure that emergency call testing is completed in line with this; and

ii) it has sufficient oversight of its network operations to enable it to identify and escalate issues affecting emergency call access.

1.10 Ofcom has decided to impose a penalty of £24,500 on Vonage for its contravention of GC3.1(c). This figure includes a 30% discount applied to the penalty figure of £35,000 we would otherwise have imposed, as a result of Vonage admitting liability and entering into a settlement with Ofcom.

[4] Vonage's Incident Report submitted to Ofcom under section 105B of the Act, dated 25 January 2018. A copy of the Incident Report is available at Annex 3.

1.11 Ofcom's view is that this penalty 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 and 3, and Annexes 1 and 2, of this document, together with Ofcom's published penalty guidelines (the Penalty Guidelines[5]). The basis for Ofcom's view as to the penalty amount is explained further in Section 4.

1.12 In light of our finding in relation to GC3.1(c), and having considered our enforcement guidelines, we do not consider it appropriate or proportionate for us to investigate any further potential breach of GC3.1(a) or section 105A of the Act at this time. In reaching this view, we weighed the likely benefits of investigating whether further breaches of GC3.1(a) and/ or section 105A could be established, against the resources that would be required for such an investigation and the comparative benefits of using those resources in other ways.[6]

[5] Ofcom's Penalty Guidelines are available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0022/106267/Penalty-Guidelines-September-2017.pdf

[6] See Ofcom's Enforcement Guidelines, page 6: https://www.ofcom.org.uk/__data/assets/pdf_file/0015/102516/Enforcement-guidelines-for-regulatory-investigations.pdf

2. Relevant facts

Introduction

2.1 This section sets out our understanding of the relevant facts from the evidence we have gathered in our investigation. We set out in Section 3 why our assessment of the evidence gives us reason to believe that Vonage has contravened GC3.1(c).

Access to the emergency organisations in the UK

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

2.3 In the UK, a person may make an emergency call, free of charge, using the national telephone numbers 999 or 112. Calls are routed between CPs in order to reach the emergency call handling agent via network interconnections. At the time of the Incident, Vonage interconnected with [✂][7] for the routing of emergency calls in the UK.

Call interconnection between Vonage and [✂ its interconnect partner]

2.4 Vonage offers voice over internet protocol (VoIP) telephony services to both business and residential customers, it has a UK customer base of approximately [✂].[8] Prior to the Incident, Vonage presented all (both emergency and non-emergency) UK calls to [✂ its interconnect partner] for onward connection.

The Incident

2.5 On 9 January 2018, following Vonage's decision to amend its call format to present calls in an ITU-T E.164 format[9] with a "+" prepended, an internal request for the change to be made was submitted to the [✂].[10] The [✂] was responsible for implementing the change.

2.6 The formatting change was implemented on 17 January 2018 at 06.00. It was a change to the signalling information, which added a '+' prefix to the dialled number on all outbound traffic sent to [✂ Vonage's interconnect partner] for termination and onward routing (the "Profile Change"). The purpose of this change was to ensure that Vonage's calls were being presented in the same format as [✂ its interconnect partner's] calls, to enable successful

[7] [✂].
[8] As detailed in the Incident Report.
[9] Recommendation ITU-T E.164 "The international public telecommunication numbering plan" provides the number structure and functionality for numbers used for international public telecommunication, detailing the components of the numbering structure and the digit analysis required to successfully route calls. https://www.itu.int/rec/T-REC-E.164/en
[10] See Annex 4, Document 1(a).

termination of all Vonage calls which were routed via the [✂ interconnect partner's] network.[11]

2.7 Prior to implementing the change Vonage completed testing, [✂], to ensure that calls to both European and UK numbers were completing successfully. Testing was completed by making calls to UK and International numbers to ensure European calls were being routed directly to [✂ Vonage's interconnect partner]. However, short codes, including the emergency call numbers 999 and 112, were not tested as part of this process.[12]

2.8 On 22 January 2018 at 12:02, Vonage received a customer complaint, which alerted it to the fact that 999 and 112 services were unavailable on the Vonage network. An investigation into the root cause was initiated and identified that the cause of the failure was that, following the implementation of the Profile Change, when short digit codes were delivered to [✂ Vonage's interconnect partner] with a "+" prepended, the calls were being rejected by [✂ its interconnect partner]and could not therefore be successfully completed. [13]

2.9 On 22 January at 19:00, Vonage rolled back the change (i.e. removed the '+' prefix) which enabled calls to short digit codes, including 999 and 112, to be completed successfully.[14]

2.10 The Incident impacted Vonage's entire UK base, therefore approximately [✂] phone lines were unable to contact the emergency services during the Incident. A total of [✂] attempts to dial 999 were made by [✂] unique customers during the Incident. [15] There was also one attempt to dial 195, directory enquiries for blind/ disabled users.[16]

Vonage's response to the Incident

2.11 As mentioned above, Vonage rolled back the Profile Change at 19:00 on 22 January 2018. This meant that access to the emergency services was restored on Vonage's network approximately 5.5 days after the Incident began. This was 6 hours and 58 minutes after Vonage became aware that emergency calls were unavailable on its network.

2.12 Following the Incident, Vonage has made further changes to its network to minimise the risk of a similar incident occurring in future. The changes made include:

- the revision of the processes associated with request, testing, implementation and verification of changes to voice services;
- the use of a dedicated [✂ interconnect partner] trunk for emergency calls, to enable Vonage to monitor the volume of emergency calls; and
- the introduction of processes to ensure that emergency calling issues can be identified and escalated.

[11] As set out in the internal request sent to the[✂]. See Annex 4, Document 1(a).
[12] See Annex 4, Document 4(a).
[13] As detailed in the Incident Report.
[14] As detailed in the Incident Report.
[15] As detailed in the Incident Report.
[16] See Annex 4, Document 10.

3. Analysis and evidence of contravention

Introduction

3.1 This section sets out our reasons, including the evidence on which we rely, for concluding that Vonage 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 06.00 on 17 January 2018 to 19.00 on 22 January 2018 as part of the publicly available telephone service that they offered.

Summary

3.2 The particularly high standard imposed by GC3.1(c) reflects the fact that telephone access to emergency organisations is of the utmost importance to public health and security. As such, we expect CPs to have done everything they possibly can to ensure that their customers have uninterrupted access to emergency organisations.[17]

3.3 We consider that appropriate testing and monitoring of a CPs' emergency call service are necessary and important measures that CPs should be taking, particularly when making changes to their network routing which could impact the availability of their emergency call service.

3.4 We have found that Vonage did not have appropriate testing and monitoring in place for its emergency call service at the time of the Incident as:

a) despite the fact Vonage had a policy in place to test emergency calls when completing a significant routing change, it failed to take sufficient steps to ensure that emergency call testing was completed. This failure was particularly serious as it meant that no emergency call testing was completed in relation to the routing change that led to the Incident and ultimately led to Vonage's emergency call service failing;

b) at the time of the Incident it did not have separate monitoring in place for its emergency call traffic which meant it was unaware that its emergency call service was unavailable for approximately 5.5 days; and

c) it would have been possible and proportionate for Vonage to have taken further steps to ensure that emergency call testing was completed when implementing the change and to have had emergency call monitoring in place for its emergency call service.

3.5 We consider that taking steps to ensure that a policy is being correctly followed is both an important and necessary part of any process, particularly where the routing and configuration of emergency calls is concerned. Further, if Vonage had carried out emergency call testing following implementation of the change in line with its policy, the Incident would have been avoided. Where the lack of emergency call monitoring is

[17] The regulatory framework for this investigation can be found at Annex 1.

concerned, we consider that, while it was not the cause of the Incident, it contributed to the prolonged duration of the Incident.

3.6 Consequently, we conclude that, in failing to have appropriate testing and monitoring in place for its emergency call service at the time of the Incident, Vonage failed to meet the requirements to take all necessary measures to maintain, to the greatest extent possible, uninterrupted access to emergency organisations in contravention of GC3.1(c).

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

Contravention of GC3.1(c)

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

3.9 For the purposes of GC3.1(c), a CP includes a person who provides publicly available telephone services.[18] Vonage provides Voice over Internet Protocol (VoIP) telephony services to business and residential customers to enable them to make and receive calls. It is therefore subject to the requirements of GC3.1(c) in relation to those publicly available telephone services it provides.

Approach to assessing compliance with GC3.1(c)

3.10 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 any publicly available telephone services that they offer. We have considered what is required by these provisions in the context of the Incident.

3.11 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 their customers have uninterrupted access to emergency organisations.

3.12 In particular, we consider that CPs should ensure that their change implementation processes include emergency call testing and that all possible steps are taken to ensure that testing is completed. Further, CPs should ensure their monitoring procedures enable them to maintain sufficient oversight of their network operations and to identify and escalate issues affecting emergency calls access as appropriate. We consider that these are necessary and important measures that CPs should be taking when making changes which could impact the availability of emergency calls on their networks as they will help to

[18] "Publicly Available Telephone Service" is defined in Part 1 of the General Conditions as meaning a service made available to the public for originating and receiving, directly and indirectly, national or national and international calls through a number or numbers in a national or international telephone numbering plan.

ensure that any changes made on their networks will not affect or interrupt citizens' access to the emergency organisations. We say this because:

i) emergency call testing enables CPs to assess the impact that a change has, or will have, on their ability to maintain uninterrupted access to emergency organisations. Therefore, where a change has been identified as potentially affecting access to the emergency services, we would expect CPs to have a process in place to include the completion of emergency call testing and to take all possible steps to ensure that this testing is completed; and

ii) although emergency call monitoring does not prevent interruption to access to the emergency services, it does enable CPs to identify and take steps to address any issues affecting access to emergency organisations on their network. Consequently, where feasible, we expect CPs to have sufficient oversight of their network operations to be able to identify and escalate issues when emergency calls are not being routed or connected correctly.

3.13 In order to inform our assessment of whether Vonage has complied with GC3.1(c), we have considered the extent to which:

a) Vonage's processes at the time of the Incident included emergency call testing and what steps were taken to ensure this testing was completed;

b) Vonage had sufficient oversight of its network operations at the time of the Incident to enable it to identify and escalate issues when emergency calls were not being routed or connected correctly.

3.14 In light of the above considerations, we then go on to consider whether Vonage failed to meet its obligation to take all necessary measures, to the greatest extent possible, to maintain uninterrupted access to emergency organisations.

(a) The extent to which Vonage's processes included emergency call testing and what steps were taken to ensure this testing was completed

3.15 As part of Ofcom's information gathering, we requested Vonage to provide any documentation setting out the processes it had in place for implementing a formatting change like the Profile Change (e.g. internal test plans, process guides, documents setting out review and sign off responsibilities).[19]

3.16 In response to this question Vonage provided a screenshot of its call routing change policy,[20] taken from [✂].[21] The text reads:

[19] See Annex 2 for further details as to Ofcom's Investigation and information gathering.
[20] See Annex 4, Document 2(a).
[21] See Annex 5, Response to Question 2(i).

"Validation of Emergency Services are REQUIRED after any change to call routing. Test calls to emergency services are to be made and call records validated."

3.17 Vonage explained that [✂] is available to all Vonage employees via [✂],[22] and any person implementing a change like the Profile Change would be expected and required to be familiar with Vonage's procedures.[23]

3.18 Vonage's policy therefore included a requirement to complete emergency call testing. This indicates there was an intention for test calls to the emergency services to be completed when implementing a change in call routing.

3.19 However, despite this, it is clear from the test call log[24] that the [✂] [25] did not complete any test calls to the emergency numbers 999 or 112 prior to implementing the Profile Change. We note that the Incident Report also states that short codes (including emergency codes) were not tested.[26] We therefore consider that Vonage did not take sufficient steps to ensure that emergency call testing was completed. We say this because:

i) the requirement to complete emergency call testing as part of the change implementation process, was written in a single sentence on Vonage's [✂]system. Although Vonage has said that anyone implementing a change like the Profile Change is 'required to be familiar' with the system, it is unconnected from the actual process of completing the testing. There appear to be no further prompts or signposts in the process to ensure that the change implementor knew or was reminded to complete emergency call testing; and

ii) the process did not require any checks to be completed to verify that emergency call testing had been completed (for example a peer review process or a senior review process).

3.20 The effect of this is that Vonage's process was reliant on a single individual (the change implementor) knowing there was a policy for emergency test calls and then carrying it out. This meant that when the [✂]failed to complete emergency call testing, this was not picked up on and therefore no testing was completed either prior to or after implementing the Profile Change.

3.21 The failure to test emergency calls when implementing the Profile Change meant that Vonage were unaware that the routing change on its network was going to make its emergency call service fail, and ultimately led to the Incident occurring.

3.22 Given the importance of emergency call access and the fact that the process called for testing to be completed, we consider that it would have been both possible and proportionate for Vonage to have taken further steps to ensure that emergency call testing

[22] See Annex 5, Response to Question 2(ii).
[23] See Annex 5, Response to Questions 2(iii).
[24] See Annex 4, Document 4(a).
[25] [✂].
[26] See the Incident Report, Annex 3. We note that the [✂]did make non-emergency test calls to ensure European calls were being routed directly to [✂its interconnect partner]. The engineer completed testing by making calls to numbers in the UK and European capitals [✂].

was completed when implementing the change. For example, the process could have required:

i) suitable checks to verify that emergency call testing had been conducted successfully; and

ii) prompts and or sign posts could have been included in the system used by the change implementor as a reminder to complete testing.

3.23 We note that peer review is now explicitly described in the [✂] document that Vonage has produced subsequent to the Incident.[27]

3.24 We consider that taking steps to ensure an emergency call testing policy is being correctly followed is both an important and necessary part of any process involving the routing and configuration of emergency calls. Therefore, checking that such processes are indeed being followed, cannot be simply taken for granted or assumed to have occurred just because the process exists, and it is particularly important where emergency calls are concerned.

3.25 Consequently, we consider that although Vonage's processes did include a requirement to test emergency calls, there are further steps that Vonage could have reasonably taken to ensure that testing was completed.

(b) The extent to which Vonage had sufficient oversight of its network operations to enable it to identify and escalate issues when emergency calls were not being routed or connected correctly

3.26 As part of our information gathering, we requested any documentation setting out the measures Vonage had in place at the time of the Incident to monitor the conveyance of Vonage's call traffic for any incidents relating to the security and/or availability of this traffic.

3.27 In response to this, Vonage provided documentation that sets out the regular and emergency services monitoring in the UK as it exists today, but with new processes that have been put in place since the Incident highlighted.[28]

3.28 This document shows that, at the time of the Incident, Vonage monitored its voice call traffic in the following ways:

a) evaluating events against defined alerting thresholds, and sending alerts where events were in breach of thresholds;[29]

b) polling, to ensure that servers and processes were up and running;[30] and

[27] See Annex 4, Document 2(b)-2.
[28] See Annex 4, Document 5(a).
[29] See Annex 4, Document 5(a), page 6.
[30] See Annex 4, Document 5(a), page 8.

c) graphing call data, to enable investigation and analysis of call trends.[31]

3.29 Vonage did therefore maintain oversight of its network to help it identify where calls were not being routed or connected correctly. However, we do not consider that this oversight was sufficient to enable it to identify and escalate issues when its emergency calls were not being routed or connected correctly.

3.30 We say this because, the documentation Vonage provided also shows that, at the time of the Incident, Vonage did not monitor its emergency call traffic separately from the rest of its voice call traffic. [32] Emergency call traffic only makes up a fraction of Vonage's overall voice call traffic and therefore the reduction in calls of [✂] emergency calls per hour[33] during the Incident was not identified by the monitoring it had in place.

3.31 As a result, the monitoring that Vonage had in place was not sufficient to pick up on the fact its whole emergency call service failed for a period of approximately 5.5 days. This meant that Vonage was unaware that its customers were unable to contact the emergency services on 999 or 112 during this period. Vonage only became aware of its emergency call service failing when it received a customer complaint concerning the unavailability of 999 and 112 at 12.02pm on 22 January 2018.[34]

3.32 It is our view that it would have been possible and proportionate for Vonage to have had further monitoring in place at the time of the Incident to enable it to identify issues affecting its emergency call traffic specifically. We say this because:

a) Vonage has informed us that following the Incident, it has moved UK emergency calls to a dedicated [✂ interconnect partner]trunk to enable monitoring and alerting of emergency calls issues.[35] The fact that it was possible for Vonage to introduce measures to monitor emergency calls shortly after the Incident, indicates that there was no technical reason why these measures were not in place prior to the Incident; and

b) Vonage has a subscriber base of approximately [✂]customers, and during the 5.5 days of the Incident there were a total of [✂]attempts to contact the emergency services by [✂]unique customers.[36] Based on these figures, an average of approximately [✂15 -60] emergency calls are made on the Vonage network each day. In light of this volume and the importance of these calls, we consider it would be proportionate for Vonage to have had specific emergency call monitoring in place and the fact they did not represents a deficiency in its processes.

3.33 Given the above, although Vonage did have some measures in place to monitor voice call traffic, we consider it would have been both possible and proportionate for Vonage to

[31] See Annex 4, Document 5(a), page 9.
[32] See Annex 4, Document 5(a) and Annex 5, Response to Question 9.
[33] This is based on [✂] calls having been attempted during the period of the Incident, see Vonage First Response, Document 10, divided by 133, which is the duration of the Incident in hours.
[34] The Incident Report, page 2.
[35] See Annex 4, Document 5(a).
[36] See Annex 4, Document 10.

have had specific emergency call monitoring in place. This would have ensured that it had sufficient oversight of its network operations to enable it to identify and escalate issues affecting the routing of emergency calls. Consequently, we do not consider that Vonage had sufficient oversight of its network where emergency calls issues were concerned.

Conclusions on a breach of GC3.1(c)

3.34 Given our findings above, we have considered whether this is sufficient for Vonage to have failed to meet its obligation to take all necessary measures, to the greatest extent possible, to maintain uninterrupted access to emergency organisations.

3.35 Having done so, we are satisfied that Vonage did fail in this respect because:

a) despite the fact it had a policy to test emergency calls when completing any significant routing change, it failed to take sufficient steps to ensure that this testing was completed. This failure was particularly serious as it meant that no emergency call testing was completed in relation to the routing change that led to the Incident and ultimately led to Vonage's emergency call service failing; and

b) at the time of the Incident it did not have sufficient oversight of its emergency call traffic which meant Vonage was unaware that its emergency call service had failed for approximately 5.5 days until it was highlighted to them by a customer complaint; and

c) it would have been possible and proportionate for Vonage to have taken further steps to ensure that emergency call testing was completed when implementing the change and to have had emergency call monitoring in place for its emergency call service.

3.36 By failing to take these measures, Vonage put uninterrupted access to the emergency services on 999 and 112 for its end-users at unnecessary risk. We consider that the failure to test emergency calls led to the Incident and the failure to monitor emergency calls lengthened the duration of the Incident. This resulted in Vonage users being unable to access the emergency organisations via "999" or "112" for a period of approximately 5.5 days.

3.37 Given this, we find that Vonage contravened its obligations under GC3.1(c) throughout the period of the Incident, which began on 17 January 2018 at 06.00 and ended on 22 January at 19.00.

3.38 For the reasons set out in Annex 1, in light of our finding in relation to GC3.1(c), we do not consider it appropriate or proportionate to investigate any further potential breaches of GC3.1(a) and/ or section 105A of the Act at this time.

4. Penalty

Summary

4.1 Ofcom has decided to impose a penalty of £24,500 on Vonage for its contravention of GC3.1(c). This figure includes a 30% discount applied to the penalty amount as a result of Vonage admitting liability and entering into a settlement agreement with Ofcom. We are also requiring Vonage to take steps to comply with the requirements of GC3.1 (c) (to the extent it has not already done so).

4.2 In reaching this decision, Ofcom has had regard to the need to incentivise CPs to comply with their regulatory obligations and is guided by our principal duty to further the interests of citizens in relation to communications matters; and to further the interests of consumers in relevant markets, where appropriate by promoting competition. In setting a penalty that would achieve this objective, we considered a number of factors in the round.

4.3 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 Vonage's failure to test whether the Profile Change would impact access to the emergency organisations on its network, led to a breach of GC3.1(c). Furthermore, it is our view that the lack of appropriate emergency call monitoring contributed to the long duration of the Incident, which further increases its seriousness.

4.4 In mitigation, we have taken into account Vonage's prompt action to restore access to the emergency organisations on its network once it became aware of the issue, and the measures it has introduced to avoid the occurrence of a similar issue on its network. Vonage also reported the Incident to Ofcom as required under section 105B and has cooperated fully with us throughout the investigation.

Consideration of whether to impose a penalty

4.5 GC3.1(c) imposes strict standards on CPs. As such we expect a CP to be able to demonstrate that it has done everything it possibly can to ensure that their customers have uninterrupted access to emergency organisations via the 999 and 112 numbers. As set out in Section 3 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.

4.6 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.

4.7 In this case, Vonage does not appear to have acted deliberately or recklessly. However, it's failure to test emergency calls led to its whole customer base being unable to access emergency organisations for approximately 5.5 days.

4.8 There existed the potential for significant harm to public health and security as a result of this failure. Further, the lack of sufficient oversight of its network operations to enable it to identify and escalate issues when emergency calls were not being routed or connected correctly, meant that the Incident continued for a longer period of time than would otherwise have been the case.

4.9 In light of the individual circumstances of this case, and for all the reasons set out in this document, we consider a financial penalty is appropriate and a proportionate response to the nature and seriousness of Vonage's contraventions. It would also help to secure Ofcom's principal duty by incentivising CPs to comply with their regulatory obligations

Level of Penalty

4.10 In considering the level of penalty which should be applied Ofcom considered the relevant statutory obligations, Vonage's relevant turnover and our Penalty Guidelines.

Statutory provisions

4.11 Section 96A of the Act provides for Ofcom to issue a notification where we have reasonable grounds to believe a person has contravened any of the General Conditions of Entitlement set under section 45 of the Act. Amongst other things, that notification can specify any penalty that Ofcom is minded to impose in accordance with section 96B[37] and must specify a period within which the person notified may make representations in response.

4.12 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.

4.13 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.

4.14 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.

[37] Section 96A(2)(e) of the Act.

4.15 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 14 September 2017.[38]

Relevant turnover

4.16 As mentioned above, under section 97 of the Act, the statutory maximum penalty Ofcom may impose on Vonage is ten per cent of its turnover for its relevant business for the period 1 April 2017 to 31 March 2018.[39]

4.17 Vonage has told us that the turnover of its relevant business for the period 1 April to 31 March 2018 was £[✂].[40] The maximum penalty Ofcom could impose on it would therefore be £[✂].

The Penalty Guidelines and relevant factors

4.18 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.[41] 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 deterrence. 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 Vonage'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 and duration of the contravention;

ii) the degree of harm, whether actual or potential, caused by the contravention, including any increased cost incurred by consumers or other market participants;

iii) any gain (financial or otherwise) made by Vonage as a result of the contravention;

iv) whether in all the circumstances, Vonage took appropriate steps to prevent the contravention;

[38] Ofcom's Penalty Guidelines. S.392 Communications Act 2003, Guidelines, 3 December 2015. Available at https://www.ofcom.org.uk/__data/assets/pdf_file/0022/106267/Penalty-Guidelines-September-2017.pdf
[39] Section 97(5)(a) of the Act.
[40] Vonage's 26 October 2018 Response to Ofcom's 3rd Notice requiring the provision of specified information under section 135 of the Communications Act 2003 dated 19 October 2018, page 1. See Annex 6.
[41] Ofcom's Penalty Guidelines, Paragraph 1.11.

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

vi) whether the contravention in question continued, or timely and effective steps were taken to end it, once Vonage became aware of it;

vii) any steps taken for remedying the consequences of the contravention;

viii) whether Vonage has a history of contraventions (repeated contraventions may lead to significantly increased penalties); and

ix) the extent to which Vonage has cooperated with our investigation.

4.19 This is the third case where Ofcom has investigated an alleged breach of GC3.1(c).[42] We have therefore had regard to the precedents set by these investigations, though we note that, we may depart from these precedents depending on the facts and the context of each case.[43]

4.20 We have also had regard to the need for transparency in applying our Penalty Guidelines, particularly as regards the weighting of the factors considered in taking our proposed approach. We explain below the weight we have ascribed to particular points.

Seriousness and duration

4.21 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 services 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. 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.

4.22 We found that, despite the fact Vonage had a policy in place to test emergency calls when completing a significant routing change, it did not take sufficient steps to ensure that emergency call testing was completed. This failure was particularly serious as it meant that no emergency call testing was completed in relation to the routing change that led to the Incident and ultimately led to Vonage's emergency call service failing.

4.23 We also found that at the time of the Incident, Vonage did not have sufficient oversight of its emergency call traffic which meant that Vonage was unaware that its emergency call service had failed for its whole subscriber base of [✂] lines until it was highlighted to them by a customer complaint. Consequently, it took approximately 5.5 days for access to emergency organisations to be restored on the Vonage network.

[42] Ofcom's own-initiative investigation into Three concerning compliance with Section 105A(1) – (3) of the Act and GC3.1 and Ofcom's own-initiative investigation into KCOM Group concerning its compliance with Section 105A(1) – (3) of the Act and GC3.1. See Ofcom's Competition and Consumer Enforcement Bulletin for further details of these investigations: https://www.ofcom.org.uk/about-ofcom/latest/bulletins/competition-bulletins/all-closed-cases

[43] Ofcom's Penalty Guidelines, Paragraph 1.14.

4.24 Further, we found that, it would have been possible and proportionate for Vonage to have taken further steps to ensure that emergency call testing was completed when implementing the change and to have had emergency call monitoring in place for its emergency call service.

4.25 For these reasons, we conclude that Vonage breached GC3.1 by failing to take all necessary measures to maintain uninterrupted access to emergency organisations in respect of the Incident. Ofcom considers this contravention of GC3.1 by Vonage to be inherently serious for the reasons discussed above.

4.26 We consider that the duration of the Incident was significant and prolonged, and we have taken this into account when considering the level of penalty to impose. However, we also take account of Vonage's prompt action to restore access to emergency organisations on its network, once it became aware of the failure, and the measures it has introduced to prevent a similar incident occurring on its network, as mitigating factors at paragraphs 4.35 and 4.36 below.

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

4.27 The potential consequences of delay in reaching emergency organisations may be severe for citizens and consumers, resulting in life-threatening situations. Consequently, any failure on the part of a CP, which leads to a situation where emergency organisations are inaccessible on a CP's network would tend to increase the level of any penalty set by Ofcom, due to the potential for such failures to give rise to significant consumer harm.

4.28 We set out above that Vonage's failure to test whether the profile change would impact on emergency calls led to its customers being unable to access the emergency organisations via 999 and 112, in contravention of GC3.1(c). We consider that this contravention had the potential to cause significant harm to Vonage's customers. In particular:

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

b) even in circumstances where any delay in contacting emergency organisations does not contribute to any actual physical harm suffered by an individual, we consider it highly likely that an inability to reach emergency organisations by calling 999 or 112 in the event of an emergency would cause emotional distress.[44]

[44] The evidence provided by Vonage in relation to the number of attempts to dial emergency organisations (See Annex 4, document 10) supports this view. In particular, it suggests that a number of customers repeatedly attempted to dial 999 during the period of the Incident, which is consistent with increasing anxiety on the part of callers.

Steps taken by Vonage to prevent the contravention and the extent to which it occurred deliberately or recklessly

4.29 There is no evidence that Vonage deliberately or recklessly contravened its obligations under GC3.1(c). Indeed, Vonage has emphasised that it recognises the importance of providing reliable access to emergency services.[45]

4.30 As set out above, Vonage's [✂],[46] included a requirement to carry out emergency call testing following any routing change which may impact emergency calls. Nevertheless, as set out in section 3, we consider that Vonage should have taken further steps to ensure that emergency call testing was completed.

4.31 Further, as noted in section 3, although Vonage did have some monitoring in place to maintain oversight of its network and identify any significant failures, the monitoring thresholds which were in place were not sufficiently granular to identify emergency call failures. Ofcom considers that Vonage's failure to include specific emergency call monitoring within its network monitoring was a significant oversight.

4.32 While we are not able to establish the lack of foresight concerning emergency call monitoring was reckless, we consider that it was careless and fell short of the standard we expect CPs to meet in discharging their obligations under GC3.1(c) by a considerable degree.

4.33 As we note in section 3, we do recognise that the monitoring would not have prevented the Incident from occurring, but we do consider that the lack of monitoring exacerbated the duration of the Incident.

Steps taken by Vonage to end the contravention

4.34 In order to resolve the Incident, Vonage rolled back the change by removing the "+" which was prepended to the number in the request line, after which [✂ its interconnect partner] was able to complete calls to short digit codes. [47] Access to the emergency organisations via the short codes 999 and 112 was restored on the Vonage network at 19.00 PM on 22 January. This was 6 hours and 58 minutes after Vonage was made aware of the issue via a customer complaint.

4.35 We consider therefore that, despite the delay in becoming aware of the issue, once it did become aware of the issue, Vonage took timely and effective steps to restore service.

4.36 We also note that it has proactively updated its call routing change policy following the event. The most notable updates to the policy's requirements are:

- review of call routing changes in a 'Core Voice Sync-up' meeting prior to change implementation to ensure that the engineer responsible for carrying out the change is aware of the steps they will be taking to implement the change;

[45] Vonage letter to Ofcom, 20 March 2018. Annex 7.
[46] See Annex 4, Document 2a.
[47] As set out in the Incident Report.

- confirmation email to be sent by the engineer to the team stating that the test call validation plan has been followed, providing examples and comments; and
- peer review of the change by the secondary on call engineer following change implementation.[48]

History of contraventions

4.37 Ofcom has not previously issued a Notification to Vonage under s96A of the Act.

4.38 The Investigation was triggered by Vonage's notification to us of the Incident, in accordance with its obligations under section 105B of the Act. Since the Incident, Vonage has provided us with information in a timely manner and has cooperated fully with the Investigation.

Incentivising compliance

4.39 We explain in our Penalty Guidelines that

> "the central objective of imposing a penalty is deterrence. The level of the penalty must be sufficient to deter the business from contravening regulatory requirements, and to deter the wider industry from doing so."

4.40 Having considered all of the circumstances of the case in the round, it appears to us that the breach was not deliberate or reckless. Neither does it appear that Vonage made any gain (financial or otherwise) from its non-compliance. Nevertheless, as we note above, we do consider that the failure to ensure that emergency call testing was completed, as its processes required, coupled with insufficient network oversight, which was caused by the lack of specific emergency call monitoring, meant that Vonage failed to take all necessary measures to provide uninterrupted access to the emergency organisations.

4.41 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 consider it appropriate to impose a penalty that takes account of the fact that this appears not to have been a deliberate breach, but that is also at a level that will incentivise Vonage and the wider industry to ensure that they comply with the requirements of GC3.1(c) at present, and on an ongoing basis.

Ofcom's conclusions on the penalty amount

4.42 Considering all the above factors in the round, the penalty we have decided to impose on Vonage is £24,500. Given that Vonage has admitted liability and entered into a settlement with Ofcom, a 30% discount has been applied to the penalty of £35,000 which we would otherwise have set.

4.43 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:

[48] See Annex 4, Document 2(b)-1.

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

4.44 Ofcom considers that the level of penalty 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 Vonage's cooperation and the fact that it 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.

Actions required of Vonage

4.45 The steps which Vonage now needs to take, to the extent it has not already taken them, to comply with the obligation in GC3.1(c) are:

a) ensure that its change implementation processes include emergency call testing and that all possible steps are taken to ensure that emergency call testing is completed in line with this; and

b) ensure it has sufficient oversight of its network operations to enable it to identify and escalate issues affecting emergency call access.

List of Annexes

Annex 1	Regulatory Framework
Annex 2	The Investigation
Annex 3	[✂]
Annex 4	[✂]
Annex 5	[✂]
Annex 6	[✂]
Annex 7	[✂]
Annex 8	[✂]

A1. Regulatory Framework

Introduction

A1.1 This section sets out the legal framework relevant to our investigation. It looks at the regulatory obligations that apply to CPs in relation to the proper and effective functioning of the network and the provision of uninterrupted access to emergency organisations. In addition, it includes 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

A1.2 The General Conditions of Entitlement place specific obligations on CPs relating to the functioning and availability of their networks, as well as the provision of access to emergency organisations.

A1.3 The obligations, set out in GC3.1,[49] which was introduced on 23 May 2011, 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.

A1.4 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."*

Sections 105A to 105D

A1.5 In addition to the provisions set out above in relation to the proper and effective functioning of the network and 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

[49] Ofcom published revised General Conditions on 19 September 2017 which came into force on 1 October 2018. Since the Incident occurred prior to 1 October 2018, the investigation was opened under the version of the conditions that applied at that date. https://www.ofcom.org.uk/__data/assets/pdf_file/0023/106394/Annex-14-Revised-clean-conditions.pdf

electronic communications networks and services. 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.

A1.6 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."*

A1.7 Ofcom has published guidance on the application of section 105A of the Act, most recently, in December 2017 (the December 2017 Guidance). Ofcom's understanding of the meaning of "security" in the context of sections 105A to 105D is expressed in the guidance as *"protecting confidentiality, integrity and availability".*[50]

A1.8 The December 2017 Guidance 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".*[51]

A1.9 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.

Ofcom's investigation and enforcement powers

A1.10 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.

A1.11 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;

[50] See "Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003", 18 December 2017, paragraph 3.2, See: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf
[51] See "Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003", 18 December 2017, paragraph 3.44, See: https://www.ofcom.org.uk/__data/assets/pdf_file/0021/51474/ofcom-guidance.pdf

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.

A1.12 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.

Focus of the Investigation

A1.13 The Incident affected the availability of access to emergency organisations on the 999 and 112 numbers, as well as the availability of access to non-emergency short code numbers such as the NHS helpline number 111. We therefore opened the investigation under the relevant provisions in GC3.1 and Section 105A of the Act.

A1.14 Owing to the importance of access to emergency organisations to safety of life, we first focused our investigation on whether there was a breach of the emergency call obligations.

A1.15 As set out above, both GC3.1(c) and section 105A contain relevant obligations in relation to emergency call access and availability. However, the obligations in GC3.1(c) are in this context more onerous than those is section 105A because of the critical nature of access to emergency services for end-users.[52] In a situation where access to emergency services has been compromised, we will therefore be concerned to ensure that a CP has met the more onerous obligations before any consideration of the broader security and protection requirements in section 105A.

A1.16 Given this, we concentrated our investigation in relation to the emergency call obligations on Vonage's compliance with GC3.1(c), during the period from 06.00 on 17 January 2018, the time the Profile Change was made and access to emergency organisations became unavailable on the Vonage network, to 19.00 on 22 January 2018, the time that access to emergency organisations was restored on Vonage's network. Our findings are set out in Section 3.

A1.17 Following our review in relation to GC3.1(c), we then went on to consider whether it would be appropriate and proportionate to investigate whether the Incident also placed Vonage

[52] 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 risks 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".

in breach of the broader access and availability obligations in GC3.1(a) and section 105A, particularly bearing in mind that the Incident did not just affect access to emergency call numbers but also access to other non-emergency short codes.

A1.18 In light of our finding in relation to GC3.1(c), we do not consider it appropriate or proportionate for us to investigate any further potential breaches at this time. In reaching this decision, we weighed the likely benefits of investigating whether further breaches of GC3.1(a) and/ or section 105A could be established, against the resources that would be required for such an investigation and the comparative benefits of using those resources in other ways.[53]

[53] See Ofcom's Enforcement Guidelines, page 6.
https://www.ofcom.org.uk/__data/assets/pdf_file/0015/102516/Enforcement-guidelines-for-regulatory-investigations.pdf

A2. The Investigation

Background

A2.1 On 25 January 2018, in accordance with section 105B of the Act, Vonage submitted an incident report to Ofcom. A copy of the incident report is attached in Annex 3.

The decision to investigate

A2.2 Typically, Ofcom receives about 700 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.[54] Ofcom considers what action to take in respect of each report that it receives, in the light of the incident reported.

A2.3 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.

A2.4 In this case, Vonage's notification under section 105B of the Act gave Ofcom cause for concern on receipt because of the particular features of the Incident that it had reported. These included:

- the complete loss of its emergency call service on 999 and 112;
- the number of lines that were affected by the loss; and
- the duration of the loss.

A2.5 Due to the impact on Vonage's services, Ofcom was particularly concerned about Vonage's procedures around testing the impact of changes on emergency calls and emergency call monitoring.

A2.6 In light of the features highlighted above, we decided that it was appropriate to open an investigation.

Information gathering

A2.7 As part of our investigation, we used our powers under section 135 of the Act to gather information from Vonage. We sent Vonage a statutory request for information under section 135 of the Act on 17 April 2018. This Notice sought information relating to its change testing and emergency call monitoring procedures. In particular, we required Vonage to provide:

i) Documentation setting out the testing Vonage had performed in respect of the Profile Change;

[54] As set out in paragraph 4.2 of the Connected Nations Report 2017 available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/108843/summary-report-connected-nations-2017.pdf

ii) Documentation setting out the governance/ approval process that was followed with respect to the implementation of the Profile Change;

iii) Documentation setting out the measures in place to monitor the conveyance of Vonage's emergency call traffic for any incidents relating to the security and/ or availability of this traffic.

iv) A copy of the most recent risk assessment/ quality assurance completed by, or on behalf of Vonage prior to the Incident, in relation to the monitoring routing or conveyance of Vonage call traffic.

A2.8 Vonage responded on 26 April 2018, and a copy of this response is at Annex 4.

A2.9 On 24 May 2018, we sent a second statutory request for information under section 135 of the Act. This Notice, sought further clarification of some of the information provided in Vonage's 26 April 2018 response.

A2.10 Vonage responded on 25 May 2018, and a copy of this response is at Annex 5.

A2.11 On 19 October 2018, we sent a third statutory request for information under section 135. This Notice, requested information from Vonage in respect of its turnover for its relevant business for the period 1 April 2017 to 31 March 2018.

A2.12 Vonage responded on 26 October 2018, and a copy of this response is at Annex 6.

Ofcom's provisional notification and the settlement procedure

A2.13 On 28 November 2018, we issued a notification under section 96A of the Act ('the Section 96A Notification') to Vonage setting out our finding that there were reasonable grounds for believing Vonage had contravened GC3.1(c) during the Incident. The Section 96A Notification also specified that Ofcom was minded to impose a penalty of £35,000 on Vonage in respect of the contravention of GC3.1(c).

A2.14 On 30 November 2018, Vonage wrote to Ofcom as part of the voluntary settlement procedure it had entered into with Ofcom:

i) Admitting it had contravened GC3.1(c) as set out in the Section 96A notification;

ii) Waiving its rights to submit representations; and

iii) Confirming its recognition that the penalty imposed by Ofcom for its contravention would be £24,500 (reduced from £35,000 because of its admission).