IN THE FIRST-TIER TRIBUNAL
GENERAL REGULATORY CHAMBER
INFORMATION RIGHTS

Appeal No. EA/2016/0110

ON APPEAL FROM:

The Information Commissioner's Monetary Penalty Notice dated 24th March 2016

Appellant:	TalkTalk Telecom Group PLC
Respondent:	Information Commissioner

Heard at:	Field House, London
Date of hearing:	16 August 2016
Date of decision:	30 August 2016

Before

Angus Hamilton (Judge)

Steve Shaw

Darryl Stephenson

Representation:

For the appellant Mr Tim Morris

For the respondent Mr Robin Hopkins

Subject matter: Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)

Cases considered:

DECISION OF THE FIRST-TIER TRIBUNAL

The Tribunal dismisses the appeal.

REASONS FOR DECISION

Introduction and Legal Framework

1 The Tribunal members would say at the outset that they are grateful to the parties for significantly narrowing the issues in dispute in this case to one central point which is described below. Consequently as there was no dispute over the relevant legal framework or chronology in this matter the Tribunal has adopted the undisputed descriptions of these matters which have been set out in the Commissioner's Response to Appeal.

2 The Commissioner's case is that the monetary penalty notice in his case was imposed for a failure by TalkTalk to notify the Commissioner of a personal data breach within 24 hours after the detection of that breach, in circumstances where it was feasible for TalkTalk to have done so.

3 'Personal data breach' is defined in regulation 2 PECR as follows:

> *"personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service;*

4 Regulation 5A PECR imposes a notification requirement on 'service providers' (of which TalkTalk is one) as follows:

> *(2) If a personal data breach occurs, the service provider shall, without undue delay, notify that breach to the Information Commissioner.*
> *….*
> *(4) The notification referred to in paragraph (2) shall contain at least a description of—*
> *(a) the nature of the breach;*
> *(b) the consequences of the breach; and*
> *(c) the measures taken or proposed to be taken by the provider to address the breach.*

5 The content of the requisite notification is prescribed in Annex 1 to Commission Regulation No 611/2013 ('the Notification Regulation') as follows:

> *Section 1*
> *Identification of the provider*
> *1. Name of the provider*
> *2. Identity and contact details of the data protection officer or other contact point where more*

information can be obtained
3. Whether it concerns a first or second notification

Initial information on the personal data breach (for completion in later notifications, where applicable)
4. Date and time of incident (if known; where necessary an estimate can be made), and of detection of incident
5. Circumstances of the personal data breach (e.g. loss, theft, copying)
6. Nature and content of the personal data concerned
7. Technical and organisational measures applied (or to be applied) by the provider to the affected personal data
8. Relevant use of other providers (where applicable)

Section 2
Further information on the personal data breach
9. Summary of the incident that caused the personal data breach (including the physical location of the breach and the storage media involved):
10. Number of subscribers or individuals concerned
11. Potential consequences and potential adverse effects on subscribers or individuals
12. Technical and organisational measures taken by the provider to mitigate potential adverse effects

Possible additional notification to subscribers or individuals
13. Content of notification
14. Means of communication used
15. Number of subscribers or individuals notified

Possible cross-border issues
16. Personal data breach involving subscribers or individuals in other Member States
17. Notification of other competent national authorities

6 Article 2(2) of the Notification Regulation deals with the timing of the obligation to notify the Commissioner of the personal data breach:

> *(2) The provider shall notify the personal data breach to the competent national authority no later than 24 hours after the detection of the personal data breach, where feasible.*
>
> *The provider shall include in its notification to the competent national authority the information set out in Annex I.*
>
> *Detection of a personal data breach shall be deemed to have taken place when the*

provider has acquired sufficient awareness that a security incident has occurred that led to personal data being compromised, in order to make a meaningful notification as required under this Regulation.

7 Article 2(3) then provides for circumstances in which the service provider is unable to provide all of the information within the 24-hour time limit:

> *(3) Where all the information set out in Annex I is not available and further investigation of the personal data breach is required, the provider shall be permitted to make an initial notification to the competent national authority no later than 24 hours after the detection of the personal data breach. This initial notification to the competent national authority shall include the information set out in Section 1 of Annex I. The provider shall make a second notification to the competent national authority as soon as possible, and at the latest within three days following the initial notification. This second notification shall include the information set out in Section 2 of Annex I and, where necessary, update the information already provided.*
>
> *Where the provider, despite its investigations, is unable to provide all information within the three-day period from the initial notification, the provider shall notify as much information as it disposes within that timeframe and shall submit to the competent national authority a reasoned justification for the late notification of the remaining information. The provider shall notify the remaining information to the competent national authority and, where necessary, update the information already provided, as soon as possible.*

8 Recital 8 to the Notification Regulation deals with the meaning of 'detection':

> *Neither a simple suspicion that a personal data breach has occurred, nor a simple detection of an incident without sufficient information being available, despite a provider's best efforts to this end, suffices to consider that a personal data breach has been detected for the purposes of this Regulation. Particular regard should be had in this connection to the availability of the information referred to in Annex I.*

9 The consequences for a failure to comply with the notification provisions under PECR and the Notification Regulation are governed by regulation 5C PECR:

> *(1) If a service provider fails to comply with the notification requirements of regulation 5A, the Information Commissioner may issue a fixed monetary penalty respect of that failure.*
>
> *(2) The amount of a fixed monetary penalty under this regulation shall be £1,000.*

…

(5) A service provider may discharge liability for the fixed monetary penalty if he pays to the Information Commissioner the amount of £800 within 21 days of receipt of the notice of intent.

10 Regulation 5C further provides that, before issuing a fixed monetary penalty, the Commissioner must serve the service provider with a notice of intent containing specified particulars: see subsections (3) and (4). The particulars to be contained in the final penalty notice are set out at subsection (7).

11 By regulation 5C(8):

(8) A service provider on whom a fixed monetary penalty is served may appeal to the Tribunal against the issue of the fixed monetary penalty notice.

The Agreed Facts in this Case

12 On 16 November 2015, one TalkTalk customer (A) accidentally obtained unauthorised access to the personal data of another customer (B) and was able to see online B's name, address, telephone numbers, email addresses and date of birth. This occurred due to a problem with one of TalkTalk's mechanisms for keeping its customers' personal data secure – specifically, the password mechanism by which customers access their TalkTalk accounts online. There is no dispute that this incident constituted a 'personal data breach' for the purposes of regulation 2 PECR. A was able to notify B as A had access through the breach to B's telephone number.

13 Customer B notified TalkTalk of the personal data breach in a number of telephone calls on 16 November 2015. A number of calls had to be made as apparently the customer kept being disconnected. Although the customer's complaints were clearly logged and she was given a reference number the Tribunal were not provided with any records kept by TalkTalk of the information provided by the customer to TalkTalk.

14 The customer then wrote a detailed letter to TalkTalk on 18 November 2015. At the same time the customer raised the matter with the Information Commissioner.

15 On 20 November, the Commissioner wrote to TalkTalk about the personal data breach, enclosing B's letter of 18 November. TalkTalk acknowledged that letter by email on 20 November, via its Information Security Officer, Mike Rabbitt.

16 On 27 November, Mr Rabbitt emailed the Commissioner to say that the incident was being investigated and that the Commissioner would be notified if TalkTalk concluded that a personal data breach had occurred.

17 TalkTalk provided the requisite notification to the Commissioner on 1 December 2015.

18 The Commissioner then asked TalkTalk to explain why the personal data breach had not been reported within the 24-hour period stipulated by the Notification Regulation. The Commissioner took the view that the personal data breach should have been notified within 24 hours of the receipt of the customer's letter of 18 November or, at the latest, within 24 hours of the Commissioner's letter of 20 November. In an email on 3 December, Mr Rabbitt explained on behalf of TalkTalk that this was because 'the incident had not been reported to either the Information Security or Fraud team'.

19 The Commissioner consequently wrote to TalkTalk on 17 February 2016 enclosing a Notice of Intent to issue a fixed monetary penalty. TalkTalk provided submissions in response dated 9 March 2016. The Commissioner considered those submissions, but remained of the view that it was lawful and appropriate to issue such a penalty in this case. He therefore issued the Notice which is the subject of this appeal on 24 March 2016.

The Appeal to the Tribunal and the Questions for the Tribunal

20 On 19 April 2016 the Appellant submitted an appeal to the Tribunal (IRT).

21 The sole issue in dispute in this case is when TalkTalk could rightly be said to have 'detected' the personal data breach or to have acquired 'sufficient awareness' of the breach.

Evidence & Submissions

22 An oral hearing took place before the Tribunal on 16 August 2016. The Tribunal heard oral submissions from the representatives for TalkTalk and the Commissioner. There were no witnesses giving evidence. The Tribunal also considered the written submissions and supporting documentation provided by the parties.

23 TalkTalk's principal contention in the case was that they only 'detected' or acquired sufficient awareness of the personal data breach after they had concluded their own investigation into the issues raised by the customer. That investigation was designed to confirm that a personal data breach had in fact occurred and also to establish how it had occurred with a view to taking remedial action. TalkTalk's case was that their investigation concluded on 30 November and that the notification on 1 December was therefore within the 24 hour time limit.

24 Ancillary to this core argument TalkTalk also submitted that it was standard industry practice for a customer's complaint of a possible personal data breach to be investigated and confirmed before the Commissioner was notified. Consequently, it was the norm for notification to take place within 24 hours of the conclusion of an investigation and not within 24 hours of the receipt of a complaint. TalkTalk

suggested that the Commissioner was aware of this practice and implicitly condoned it. In this particular case reference was made to the Commissioner having a meeting with TalkTalk on 27th November (not specifically about this case) and of the case being mentioned with a TalkTalk representative saying that investigations into the matter were still ongoing. TalkTalk submitted that the lack of any negative response from the Commissioner's representatives implied that they were willing to wait until the conclusion of the investigation before any notification was given.

25 TalkTalk also referred to the number of customers it had (some 4 million) and suggested that an impractical burden would be placed on them if every complaint from a customer of a suspected personal data breach had to be treated as an established breach and notified to the Commissioner within 24 hours. No clear evidence of the incidence of complaints of personal data breached was provided by TalkTalk but under questioning from the Tribunal it was estimated that TalkTalk received approximately 50 such complaints a month. TalkTalk also pointed to the fact that this was a single complaint from one customer and was not corroborated by any other customer's experience. TalkTalk indicated that this further supported their analysis that an investigation was required before it could be said that a personal data breach had been 'detected'.

26 The Commissioner disagreed with TalkTalk's submissions based on the particular circumstances of this case: The customer did not make an unparticularised complaint or unsupported allegation. She provided a detailed account of exactly what had happened, and she provided supporting evidence to corroborate that account. In fact, she had already discussed the incident in some detail with employees of TalkTalk on 16 November, the date on which the personal data breach occurred. In those circumstances, B's communications plainly equipped TalkTalk with 'sufficient awareness'.

27 The Commissioner further submitted that 'detection' is distinct from 'conclusive confirmation'. Detection is deemed to have occurred when TalkTalk acquired 'sufficient awareness' that a personal data breach had occurred, so as to enable it to make a meaningful notification. In these circumstances – in particular, given the level of detail and supporting evidence that the customer provided on 18 November – that threshold was met well before TalkTalk concluded its internal investigations.

28 In relation to the suggestion that TalkTalk understood from a meeting with the Commissioner on 27 November 2015 that the Commissioner was content to await notification following the outcome of TalkTalk's investigation - The Commissioner stated that he had no record, nor did his officers have any recollection, of any such indication being given at the meeting of 27 November. That meeting was not about this particular incident.

29 The Commissioner submitted that the Regulations envisaged a multi stage reporting approach which suggested the gathering and provision of information to the Commissioner as it was acquired by the service provider rather than an investigation having to be fully completed before the obligation to notify the Commissioner arose. The Commissioner referred in particular to Article 2(3) which is quoted at paragraph 7 above. In the Commissioner's view, the legislation did not envisage that an investigation should be completed and then notification occurring. Rather, it envisaged as much as possible to be

provided as it became available.

30 The Commissioner invited the Tribunal to consider the information that had to be provided under Section 1 of Annex 1 to Commission Regulation No 611/2013 (paragraph 5 above) and to ask itself whether the information required in Section 1 could have been provided within 24 hours of the receipt of the customer's letter of 18th November. The Commissioner submitted that the answer to that question had to be 'yes'. In a similar vein the Commissioner also invited the Tribunal to consider the actual notification provided by TalkTalk on 1 December **[p 14 bundle]** and submitted that there was nothing in the report that could not have come from the customer's original complaint rather than a subsequent investigation.

31 The Commissioner's representative denied that the Commissioner indulged any practice whereby a service provider only notified the Commissioner of a personal data breach after conducting an investigation. If there was any significant gap between the date of the breach and the date of notification a service provider would be asked for an explanation. The Commissioner emphasised that TalkTalk had failed to provide any documentary evidence of their notifications where the Commissioner had appeared to indulge such a practice.

32 The Commissioner also relied on two ancillary points. First, the Commissioner pointed to the fact that when first asked for an explanation for the apparent late notification (in a letter dated 2 December 2015) Mr Rabbit, TalkTalk's Information Security Officer, replied that the 'incident had not been reported to either the Information Security of (*sic*) Fraud team. This was despite the facts that Mr Rabbit was the Information Security Officer and that he had previously acknowledged (in an email dated 27 November 2015) receipt of the Commissioner's letter of 20 November 2015 containing the customer's complaint. This, the Commissioner suggested, indicated a level of disorganisation rather than diligence in relation to the handling of the customer's complaint. Secondly, the Commissioner emphasised that TalkTalk had failed to adduce any evidence as to what investigatory steps it had actually undertaken between 18 and 30 November 2015. As stated in the preceding paragraph - in the Commissioner's view there was nothing in the personal data breach report of 1 December 2015 submitted by TalkTalk that flowed from an investigation rather than the customer's original complaint.

Conclusion

33 The Tribunal was unanimous in dismissing this appeal for the following reasons:

- The Tribunal considered that the level of detail in the customer's letter of 18th November led to the inevitable conclusion that there was no other explanation for what had occurred other than that there had been a personal data breach.

- The Tribunal noted that TalkTalk's representatives were not able to suggest any credible alternative scenario apart from a personal data breach that would explain the contents of the customer's letter of 18th November.

- The Tribunal consequently concluded that TalkTalk had sufficient awareness of the breach and that a personal data breach had been detected upon receipt of the customer's letter of 18th November. The Tribunal strongly suspected that TalkTalk in fact had sufficient awareness of the breach when the customer telephoned on 16th November but were hampered in reaching any conclusion on this point by the failure of TalkTalk to provide any details of that initial complaint.

- The Tribunal noted that the Regulations made no specific provision for time to conduct an investigation by a service provider beyond permitting a strictly time-limited staged notification process in certain circumstances. The Tribunal considered that to 'read in' the requirement that there should always be a period of investigation before notification risked undermining the strict time limits in the Regulations as there was no specific provision for investigations and consequently no express time limit on the conduct of such an investigation.

- The Tribunal agreed with the Commissioner's submissions that all the information that had to be provided under Section 1 of Annex 1 to Commission Regulation No 611/2013 and was provided by TalkTalk by the notification of 1 December was available to the company from the customer's letter of 18th November and that none of the provided information appeared to derive from any subsequent investigation.

- The Tribunal distinguished the facts of this current case - where the customer had provided considerable detail of circumstances that could only be explained by a personal data breach - from the situation where a customer made a generalised complaint of a suspected personal data breach - for example, a complaint about junk mail which alluded to the recipient being a TalkTalk customer. In the latter case an investigation may well be required before a personal data breach was detected. Given this distinction and given TalkTalk's own submissions that the complaints received about potential personal data breaches amounted to about 50 per month, the Tribunal were unimpressed by the contention that holding that 'sufficient awareness' in this case arose from the customer's letter would place an unreasonable burden on service providers.

- The Tribunal did not accept that the Commissioner had allowed a practice to arise whereby service providers only notified after an investigation and noted that no evidence to this effect had been provided.

Signed:

Angus Hamilton DJ(MC)
Tribunal Judge Date: 30 August 2016