PRIVACY AND ELECTRONIC COMMUNICATIONS (EC DIRECTIVE) REGULATIONS 2003

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

FIXED MONETARY PENALTY NOTICE

To: TalkTalk Telecom Group Plc

Of: 11 Evesham Street, London, W11 4AR

1. The Information Commissioner ("Commissioner") has decided to issue TalkTalk Telecom Group Plc ("TalkTalk") with a fixed monetary penalty under section 5C of the Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"). The penalty is being issued because of a contravention of regulation 5A of PECR.

2. This notice explains the Commissioner's decision.

Legal framework

3. TalkTalk is a "service provider" as defined in regulation 5(1) of PECR.

4. Regulation 5A of PECR states:

"(1) In this regulation … 'service provider' has the meaning given in regulation 5(1).

(2) If a personal data breach occurs, the service provider shall, without undue delay, notify that breach to the Information Commissioner.

(3) ..

(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. Regulation 2 of PECR defines a "personal data breach" as:

".. 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."

6. Further rules in relation to the notification of personal data breaches are set out in Commission Regulation No 611/2013 (the "Notification Regulations"). Article 2(2) of the Notification Regulations states:

"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.

..

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. Service providers must therefore notify the Commissioner within 24 hours of becoming aware that a personal data breach has occurred. There is no threshold for how serious the breach must be – all breaches must be notified.

8. Section 5C of PECR states:

"*(1) If a service provider fails to comply with the notification requirements of regulation 5A, the Information Commissioner may issue a fixed monetary penalty notice in respect of that failure.*

(2) The amount of a fixed monetary penalty under this regulation shall be £1,000.

(3) Before serving such a notice, the Information Commissioner must serve the service provider with a notice of intent.

(4) The notice of intent must –

(a) state the name and address of the service provider;

(b) state the nature of the breach;

(c) indicate the amount of the fixed monetary penalty;

(d) include a statement informing the service provider of the opportunity to discharge the liability for the fixed monetary penalty;

(e) indicate the date on which the Information Commissioner proposes to serve the fixed monetary penalty notice; and

(f) inform the service provider that he may make written representations in relation to the proposal to serve a fixed monetary penalty notice within 21 days of receipt of the notice of intent.

(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."

Background to the case

9. On 16 November 2015 customer A was able to access personal data about customer B when using TalkTalk's online "MyAccount" facility. The information disclosed was name, address, telephone and account billing information.

10. The incident was caused by a bug in the customer password reset facility which has subsequently been remedied.

11. On 18 November 2015 customer B wrote to TalkTalk to complain about the incident. The Commissioner is satisfied that the evidence provided by customer B was sufficient to have enabled TalkTalk to conclude that a security incident had occurred that led to personal data being compromised. Therefore, in accordance with Article 2(2) of the Notification Regulations, the detection of the personal data breach is deemed to have taken place on 18 November 2015. However, TalkTalk failed to notify the Commissioner of the personal data breach until 1 December 2015.

The Commissioner's decision to issue a fixed monetary penalty

12. The Commissioner is satisfied that there has been a personal data breach within the meaning of regulation 2 of PECR.

13. Further, the Commissioner is satisfied that TalkTalk has contravened regulation 5A of PECR by failing to notify the Commissioner of that personal data breach without undue delay.

14. In compliance with the procedural rights under regulation 5C of PECR, the Commissioner served TalkTalk with a notice of intent dated 17 February 2016 in which he set out his preliminary thinking. TalkTalk made representations in response to that notice of intent which have been taken into account by the Commissioner in reaching his final view.

15. The Commissioner is accordingly entitled to issue a monetary penalty in this case. He has gone on to consider whether, in the circumstances, he should exercise his discretion so as to issue a monetary penalty.

16. The Commissioner's underlying objective in imposing a monetary penalty is to promote compliance with PECR. The requirement to notify the Commissioner of personal data breaches provides an important opportunity for him to assess whether a service provider is complying with its obligations under PECR, including the duty to take appropriate technical and organisational measures to safeguard the security of its service and the duty to notify customers of breaches adversely affecting their privacy. A monetary penalty in this case would act as a general encouragement towards compliance with the requirement to notify personal data breaches, or at least as a deterrent against non-compliance, on the part of all service providers.

17. The Commissioner has therefore decided to impose a fixed monetary penalty on TalkTalk for failing to comply with the notification requirements of regulation 5A of PECR. The Commissioner considers that this decision is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

18. As provided for by regulation 5C(2) of PECR, the amount of that penalty will be **£1000 (one thousand pounds)**.

Conclusion

19. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 27 April 2016 at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

20. There is a right of appeal to the First-tier Tribunal (Information Rights) against the imposition of the fixed monetary penalty. Any notice of appeal should be received by the Tribunal within 28 days of the date of this fixed monetary penalty notice. Information about appeals is set out in Annex 1.

21. In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court of any sheriffdom in Scotland.

Dated the 24th day of March 2016

Signed: ……..

Stephen Eckersley
Head of Enforcement
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1 - RIGHT OF APPEAL

1. Regulation 5C(8) of PECR gives any person upon whom a fixed monetary penalty notice has been served a right of appeal to the (First-tier Tribunal) General Regulatory Chamber (the 'Tribunal') against the notice.

2. If you decide to appeal and if the Tribunal considers:-

   a) that the notice against which the appeal is brought is not in accordance with the law; or

   b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

   the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.

3. You may bring an appeal by serving a notice of appeal on the Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester
   LE1 8DJ

   a) The notice of appeal should be sent so it is received by the Tribunal within 28 days of the date of the notice.

   b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);
b) an address where documents may be sent or delivered to you;
c) the name and address of the Information Commissioner;
d) details of the decision to which the proceedings relate;
e) the result that you are seeking;
f) the grounds on which you rely;
g) you must provide with the notice of appeal a copy of the monetary penalty notice;
h) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).